https://nciipc.gov.in

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16 - 30 Apr 2025 Vol. 12 No. 08

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 10web					
Product: form_maker					
Affected Version(s): * Up to (excluding) 1.15.32					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Apr-2025	4.8	The Form Maker by 10Web WordPress plugin before 1.15.32 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID: CVE-2024-10680**	N/A	A-10W-FORM-050525/1
Vendor: a-blogcms					
Product: a-blogcms					
Affected Version(s): 3.1.15					
Server-Side Request Forgery (SSRF)	17-Apr-2025	7.6	An issue in a-blogcms 3.1.15 allows a remote attacker to obtain sensitive information via the /bid/1/admin/entry-edit/ path. **CVE ID: CVE-2025-29461**	N/A	A-A-B-A-BL-050525/2
Vendor: Alkacon					
Product: opencms					
Affected Version(s): 17.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Apr-2025	6.5	Cross Site Scripting vulnerability in Create/Modify article function in Alkacon OpenCMS 17.0 allows remote attacker to inject javascript payload via image title sub-field in the image field **CVE ID: CVE-2024-42699**	N/A	A-ALK-OPEN-050525/3

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Apr-2025	5.4	A stored cross-site scripting (XSS) vulnerability in Alkacon OpenCMS v17.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the image parameter under the Create/Modify article function. **CVE ID: CVE-2024-41446**	N/A	A-ALK-OPEN-050525/4
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2025	5.4	A stored cross-site scripting (XSS) vulnerability in Alkacon OpenCMS v17.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the author parameter under the Create/Modify article function. **CVE ID: CVE-2024-41447**	N/A	A-ALK-OPEN-050525/5
Vendor: alttext					
Product: alt_text_ai					
Affected Version(s): * Up to (excluding) 1.9.94					
Missing Authorization	22-Apr-2025	4.3	Missing Authorization vulnerability in alttextai Download Alt Text AI allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Download Alt Text AI: from n/a through 1.9.93. **CVE ID: CVE-2025-46232**	N/A	A-ALT-ALT_-050525/6
Vendor: angeljudesuarez					
Product: placement_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	28-Apr-2025	7.3	A vulnerability classified as critical has been found in itsourcecode Placement Management System 1.0. Affected is an unknown function of the file /add_drive.php. The manipulation of the	N/A	A-ANG-PLAC-050525/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			argument drive_title leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well. **CVE ID: CVE-2025-4024**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	28-Apr-2025	7.3	A vulnerability classified as critical was found in itsourcecode Placement Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /registration.php. The manipulation of the argument Name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well. **CVE ID: CVE-2025-4025**	N/A	A-ANG-PLAC-050525/8
Vendor: Apache					
Product: hertzbeat					
Affected Version(s): * Up to (excluding) 1.7.0					
Server-Side Request Forgery (SSRF)	16-Apr-2025	6.5	Server-Side Request Forgery (SSRF) vulnerability in Apache HertzBeat. This issue affects Apache HertzBeat (incubating): before 1.7.0. Users are recommended to upgrade to version 1.7.0, which fixes the issue. **CVE ID: CVE-2024-56736**	https://lists.apache.org/thread/kdzg36h9yxp0q0n4lhcfppxntjy8rj1x, https://lists.apache.org/thread/lwfhsllos1rx9v8k0yhl252cbpqpn0sv	A-APA-HERT-050525/9
Vendor: appventure					
Product: dietiqa					
Affected Version(s): 1.0.20					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Apr-2025	9.8	A SQL Injection vulnerability exists in the `u` parameter of the progress-body-weight.php endpoint of Dietiqa App v1.0.20. **CVE ID: CVE-2025-28009**	N/A	A-APP-DIET-050525/10
Vendor: avecnous					
Product: event_post					
Affected Version(s): * Up to (excluding) 5.10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2025	6.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bastien Ho Event post allows DOM-Based XSS. This issue affects Event post: from n/a through 5.9.11. **CVE ID: CVE-2025-46228**	N/A	A-AVE-EVEN-050525/11
Vendor: caseproof					
Product: memberpress					
Affected Version(s): * Up to (including) 1.11.37					
Exposure of Sensitive Information to an Unauthorized Actor	22-Apr-2025	5.3	The Memberpress plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.11.37 via the WordPress core search feature. This makes it possible for unauthenticated attackers to extract sensitive data from posts that have been restricted to higher-level roles such as administrator. **CVE ID: CVE-2024-11299**	N/A	A-CAS-MEMB-050525/12
Vendor: Cminds					
Product: cm_ad_changer					
Affected Version(s): * Up to (excluding) 2.0.6					
Cross-Site Request Forgery	22-Apr-2025	4.3	Cross-Site Request Forgery (CSRF) vulnerability in CreativeMindsSolutions CM	N/A	A-CMI-CM_A-050525/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			Ad Changer allows Cross Site Request Forgery. This issue affects CM Ad Changer: from n/a through 2.0.5. **CVE ID: CVE-2025-46245**		
Product: cm_answers					
Affected Version(s): * Up to (excluding) 3.3.4					
Cross-Site Request Forgery (CSRF)	22-Apr-2025	4.3	Cross-Site Request Forgery (CSRF) vulnerability in CreativeMindsSolutions CM Answers allows Cross Site Request Forgery. This issue affects CM Answers: from n/a through 3.3.3. **CVE ID: CVE-2025-46246**	N/A	A-CMI-CM_A-050525/14
Vendor: code-projects					
Product: news_publishing_site_dashboard					
Affected Version(s): 1.0					
Improper Access Control	27-Apr-2025	6.3	A vulnerability was found in codeprojects News Publishing Site Dashboard 1.0. It has been rated as critical. This issue affects some unknown processing of the file /edit-category.php of the component Edit Category Page. The manipulation of the argument category_image leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3969**	N/A	A-COD-NEWS-050525/15
Improper Neutralization of Special Elements in Output Used by a Downstream Component	27-Apr-2025	6.3	A vulnerability was found in codeprojects News Publishing Site Dashboard 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /api.php. The manipulation of the	N/A	A-COD-NEWS-050525/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			argument cat_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3968**		
Product: online_exam_mastering_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Apr-2025	6.1	code-projects Online Exam Mastering System 1.0 is vulnerable to Cross Site Scripting (XSS) in feedback.php via the "q" parameter allowing remote attackers to execute arbitrary code. **CVE ID: CVE-2025-28121**	N/A	A-COD-ONLI-050525/17
Product: patient_record_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-Apr-2025	6.3	A vulnerability, which was classified as critical, was found in codeprojects Patient Record Management System 1.0. This affects an unknown part of the file /edit_rpatient.php.php. The manipulation of the argument id/lastname leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3955**	N/A	A-COD-PATI-050525/18
Vendor: codeastro					
Product: bus_ticket_booking_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation	28-Apr-2025	5	Cross-Site Scripting (XSS) vulnerability exists in the User Registration and User Profile features of Codeastro Bus Ticket Booking System v1.0 allows	N/A	A-COD-BUS_-050525/19

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			an attacker to execute arbitrary code into the Full Name and Address fields during user registration or profile editing. **CVE ID: CVE-2025-25776**		
Product: internet_banking_system					
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2025	6.1	Code Astro Internet Banking System 2.0.0 is vulnerable to Cross Site Scripting (XSS) via the name parameter in /admin/pages_account.php. **CVE ID: CVE-2025-29015**	N/A	A-COD-INTE-050525/20
Vendor: Codepeople					
Product: appointment_booking_calendar					
Affected Version(s): * Up to (excluding) 1.3.93					
Cross-Site Request Forgery (CSRF)	22-Apr-2025	8.2	Cross-Site Request Forgery (CSRF) vulnerability in codepeople Appointment Booking Calendar allows SQL Injection. This issue affects Appointment Booking Calendar: from n/a through 1.3.92. **CVE ID: CVE-2025-46241**	N/A	A-COD-APPO-050525/21
Missing Authorization	22-Apr-2025	5.3	Missing Authorization vulnerability in codepeople Appointment Booking Calendar allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Appointment Booking Calendar: from n/a through 1.3.92. **CVE ID: CVE-2025-46247**	N/A	A-COD-APPO-050525/22
Product: calculated_fields_form					
Affected Version(s): * Up to (excluding) 5.2.62					
Improper Neutralization of Input During Web	29-Apr-2025	3.5	The Calculated Fields Form WordPress plugin before 5.2.62 does not sanitise and escape some of its settings,	N/A	A-COD-CALC-050525/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID: CVE-2024-12273**		
Vendor: Commvault					
Product: commvault					
Affected Version(s): From (including) 11.20.0 Up to (excluding) 11.20.217					
N/A	25-Apr-2025	8.8	Commvault Web Server has an unspecified vulnerability that can be exploited by a remote, authenticated attacker. According to the Commvault advisory: "Webservers can be compromised through bad actors creating and executing webshells." Fixed in version 11.36.46, 11.32.89, 11.28.141, and 11.20.217 for Windows and Linux platforms. This vulnerability was added to the CISA Known Exploited Vulnerabilities (KEV) Catalog on 2025-04-28. **CVE ID: CVE-2025-3928**	https://documentation.commvault.com/securityadvisories/CV_2025_03_1.html, https://www.commvault.com/blogs/notice-security-advisory-update, https://www.commvault.com/blogs/security-advisory-march-7-2025	A-COM-COMM-050525/24
Affected Version(s): From (including) 11.28.0 Up to (excluding) 11.28.141					
N/A	25-Apr-2025	8.8	Commvault Web Server has an unspecified vulnerability that can be exploited by a remote, authenticated attacker. According to the Commvault advisory: "Webservers can be compromised through bad actors creating and executing webshells." Fixed in version 11.36.46, 11.32.89, 11.28.141, and 11.20.217 for Windows and Linux platforms. This vulnerability was added to	https://documentation.commvault.com/securityadvisories/CV_2025_03_1.html, https://www.commvault.com/blogs/notice-security-advisory-update, https://www.commvault.com/blogs/security-advisory-march-	A-COM-COMM-050525/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the CISA Known Exploited Vulnerabilities (KEV) Catalog on 2025-04-28. **CVE ID: CVE-2025-3928**	7-2025	
Affected Version(s): From (including) 11.32.0 Up to (excluding) 11.32.89					
N/A	25-Apr-2025	8.8	Commvault Web Server has an unspecified vulnerability that can be exploited by a remote, authenticated attacker. According to the Commvault advisory: "Webservers can be compromised through bad actors creating and executing webshells." Fixed in version 11.36.46, 11.32.89, 11.28.141, and 11.20.217 for Windows and Linux platforms. This vulnerability was added to the CISA Known Exploited Vulnerabilities (KEV) Catalog on 2025-04-28. **CVE ID: CVE-2025-3928**	https://documentation.commvault.com/securityadvisories/CV_2025_03_1.html, https://www.commvault.com/blogs/notice-security-advisory-update, https://www.commvault.com/blogs/security-advisory-march-7-2025	A-COM-COMM-050525/26
Affected Version(s): From (including) 11.36.0 Up to (excluding) 11.36.46					
N/A	25-Apr-2025	8.8	Commvault Web Server has an unspecified vulnerability that can be exploited by a remote, authenticated attacker. According to the Commvault advisory: "Webservers can be compromised through bad actors creating and executing webshells." Fixed in version 11.36.46, 11.32.89, 11.28.141, and 11.20.217 for Windows and Linux platforms. This vulnerability was added to the CISA Known Exploited Vulnerabilities (KEV) Catalog on 2025-04-28. **CVE ID: CVE-2025-3928**	https://documentation.commvault.com/securityadvisories/CV_2025_03_1.html, https://www.commvault.com/blogs/notice-security-advisory-update, https://www.commvault.com/blogs/security-advisory-march-7-2025	A-COM-COMM-050525/27
Vendor: Craftcms					
Product: craft_cms					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.9.15					
Improper Control of Generation of Code ('Code Injection')	25-Apr-2025	10	Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. Starting from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17, Craft is vulnerable to remote code execution. This is a high-impact, low-complexity attack vector. This issue has been patched in versions 3.9.15, 4.14.15, and 5.6.17, and is an additional fix for CVE-2023-41892. **CVE ID: CVE-2025-32432**	https://github.com/craftcms/cms/commit/e1c85441fa47eeb7c688c2053f25419bc0547b47	A-CRA-CRAF-050525/28
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.14.15					
Improper Control of Generation of Code ('Code Injection')	25-Apr-2025	10	Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. Starting from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17, Craft is vulnerable to remote code execution. This is a high-impact, low-complexity attack vector. This issue has been patched in versions 3.9.15, 4.14.15, and 5.6.17, and is an additional fix for CVE-2023-41892. **CVE ID: CVE-2025-32432**	https://github.com/craftcms/cms/commit/e1c85441fa47eeb7c688c2053f25419bc0547b47	A-CRA-CRAF-050525/29
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.6.17					
Improper Control of Generation of Code ('Code Injection')	25-Apr-2025	10	Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. Starting from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17, Craft is vulnerable to	https://github.com/craftcms/cms/commit/e1c85441fa47eeb7c688c2053f25419bc0547b47	A-CRA-CRAF-050525/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution. This is a high-impact, low-complexity attack vector. This issue has been patched in versions 3.9.15, 4.14.15, and 5.6.17, and is an additional fix for CVE-2023-41892. **CVE ID: CVE-2025-32432**		
Vendor: davidvongries					
Product: ultimate_dashboard					
Affected Version(s): * Up to (excluding) 3.8.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2025	3.5	The Ultimate Dashboard WordPress plugin before 3.8.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID: CVE-2025-1524**	N/A	A-DAV-ULTI-050525/31
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2025	3.5	The Ultimate Dashboard WordPress plugin before 3.8.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID: CVE-2025-1525**	N/A	A-DAV-ULTI-050525/32
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2025	3.5	The Ultimate Dashboard WordPress plugin before 3.8.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks	N/A	A-DAV-ULTI-050525/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID: CVE-2025-1523**		
Vendor: dogukanurker					
Product: flaskblog					
Affected Version(s): 2.6.1					
Cross-Site Request Forgery (CSRF)	17-Apr-2025	6.5	An arbitrary file deletion vulnerability in the /post/{postTitle} component of flaskBlog v2.6.1 allows attackers to delete article titles created by other users via supplying a crafted POST request. **CVE ID: CVE-2025-28101**	N/A	A-DOG-FLAS-050525/34
Vendor: dragonflydb					
Product: dragonfly					
Affected Version(s): * Up to (excluding) 1.27.0					
Missing Report of Error Condition	17-Apr-2025	3.3	DragonflyDB Dragonfly before 1.27.0 allows authenticated users to cause a denial of service (daemon crash) via a crafted Redis command. The validity of the scan cursor was not checked. **CVE ID: CVE-2025-26268**	https://github.com/dragonflydb/dragonfly/commit/d1fac0f912edb323a2bdd6404c518cda21eac243, https://github.com/dragonflydb/dragonfly/compare/v1.26.4...v1.27.0	A-DRA-DRAG-050525/35
Vendor: e4jconnect					
Product: vikrestaurants_table_reservations_and_take-away					
Affected Version(s): * Up to (excluding) 1.4					
Cross-Site Request Forgery (CSRF)	22-Apr-2025	7.1	Cross-Site Request Forgery (CSRF) vulnerability in e4jvikwp VikRestaurants Table Reservations and Take-Away allows Cross Site Request Forgery. This issue affects VikRestaurants Table Reservations and Take-Away: from n/a	N/A	A-E4J-VIKR-050525/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 1.3.3. **CVE ID: CVE-2025-46251**		
Vendor: fabianros					
Product: atm_banking					
Affected Version(s): 1.0					
N/A	28-Apr-2025	4.4	A vulnerability was found in code-projects ATM Banking 1.0. It has been classified as critical. Affected is the function moneyDeposit/moneyWithdraw. The manipulation leads to business logic errors. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-4037**	N/A	A-FAB-ATM_-050525/37
Vendor: foxcms					
Product: foxcms					
Affected Version(s): * Up to (including) 1.25					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Apr-2025	7.2	FOXCMS <= V1.25 is vulnerable to SQL Injection via $param['title'] in /admin/util/Field.php. **CVE ID: CVE-2025-29181**	N/A	A-FOX-FOXC-050525/38
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Apr-2025	7.2	In FOXCMS <=1.25, the installdb.php file has a time - based blind SQL injection vulnerability. The url_prefix, domain, and my_website POST parameters are directly concatenated into SQL statements without filtering. **CVE ID: CVE-2025-29180**	N/A	A-FOX-FOXC-050525/39
Vendor: GNU					
Product: mailman					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2.1.1 Up to (including) 2.1.39					
Path Traversal: '../filedir'	20-Apr-2025	5.8	GNU Mailman 2.1.39, as bundled in cPanel (and WHM), allows unauthenticated attackers to read arbitrary files via ../ directory traversal at /mailman/private/mailman (aka the private archive authentication endpoint) via the username parameter. NOTE: multiple third parties report that they are unable to reproduce this, regardless of whether cPanel or WHM is used. **CVE ID: CVE-2025-43919**	N/A	A-GNU-MAIL-050525/40
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Apr-2025	5.4	GNU Mailman 2.1.39, as bundled in cPanel (and WHM), in certain external archiver configurations, allows unauthenticated attackers to execute arbitrary OS commands via shell metacharacters in an email Subject line. NOTE: multiple third parties report that they are unable to reproduce this, regardless of whether cPanel or WHM is used. **CVE ID: CVE-2025-43920**	N/A	A-GNU-MAIL-050525/41
Incorrect Authorization	20-Apr-2025	5.3	GNU Mailman 2.1.39, as bundled in cPanel (and WHM), allows unauthenticated attackers to create lists via the /mailman/create endpoint. NOTE: multiple third parties report that they are unable to reproduce this, regardless of whether cPanel or WHM is used. **CVE ID: CVE-2025-43921**	N/A	A-GNU-MAIL-050525/42
Vendor: Google					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: chrome					
Affected Version(s): * Up to (excluding) 135.0.7049.95					
Heap-based Buffer Overflow	16-Apr-2025	8.8	Heap buffer overflow in Codecs in Google Chrome on Windows prior to 135.0.7049.95 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) **CVE ID: CVE-2025-3619**	https://chromereleases.googleblog.com/2025/04/stable-channel-update-for-desktop_15.html	A-GOO-CHRO-050525/43
Use After Free	16-Apr-2025	8.8	Use after free in USB in Google Chrome prior to 135.0.7049.95 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID: CVE-2025-3620**	https://chromereleases.googleblog.com/2025/04/stable-channel-update-for-desktop_15.html	A-GOO-CHRO-050525/44
Vendor: ibericode					
Product: html_forms					
Affected Version(s): * Up to (excluding) 1.5.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2025	6.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Link Software LLC HTML Forms allows Stored XSS. This issue affects HTML Forms: from n/a through 1.5.2. **CVE ID: CVE-2025-46236**	N/A	A-IBE-HTML-050525/45
Vendor: icegram					
Product: icegram_express					
Affected Version(s): * Up to (excluding) 5.7.50					
Improper Neutralization of Input During Web Page Generation	25-Apr-2025	6.1	The Icegram Express WordPress plugin before 5.7.50 does not sanitise and escape some of its Template settings, which could allow high privilege users such as	N/A	A-ICE-ICEG-050525/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID: CVE-2025-0671**		
Affected Version(s): * Up to (excluding) 5.7.52					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2025	3.5	The Icegram Express formerly known as Email Subscribers WordPress plugin before 5.7.52 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID: CVE-2024-11924**	N/A	A-ICE-ICEG-050525/47
Vendor: Jetbrains					
Product: rubymine					
Affected Version(s): * Up to (excluding) 2025.1					
Insecure Default Initialization of Resource	17-Apr-2025	8.3	In JetBrains RubyMine before 2025.1 remote Interpreter overwrote ports to listen on all interfaces **CVE ID: CVE-2025-43015**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-RUBY-050525/48
Product: toolbox					
Affected Version(s): * Up to (excluding) 2.6					
Cleartext Transmission of Sensitive Information	17-Apr-2025	6.9	In JetBrains Toolbox App before 2.6 unencrypted credential transmission during SSH authentication was possible **CVE ID: CVE-2025-43013**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TOOL-050525/49
Missing Critical Step in Authentication	17-Apr-2025	6.1	In JetBrains Toolbox App before 2.6 the SSH plugin established connections without sufficient user confirmation	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TOOL-050525/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-43014		
Improper Validation of Certificate with Host Mismatch	17-Apr-2025	4.2	In JetBrains Toolbox App before 2.6 host key verification was missing in SSH plugin **CVE ID: CVE-2025-42921**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TOOL-050525/51
Vendor: jsite					
Product: jsite					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2025	3.5	A vulnerability was found in baseweb JSite 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /a/sys/user/save. The manipulation of the argument Name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3788**	N/A	A-JSI-JSIT-050525/52
Vendor: Kibokolabs					
Product: watu_quiz					
Affected Version(s): * Up to (excluding) 3.4.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Apr-2025	7.6	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Bob Watu Quiz allows SQL Injection. This issue affects Watu Quiz: from n/a through 3.4.3. **CVE ID: CVE-2025-46242**	N/A	A-KIB-WATU-050525/53
Vendor: klarna					
Product: klarna_checkout_for_woocommerce					
Affected Version(s): * Up to (excluding) 2.13.5					
N/A	17-Apr-2025	7.5	The Klarna Checkout for WooCommerce WordPress plugin before 2.13.5	N/A	A-KLA-KLAR-050525/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exposes an unauthenticated WooCommerce Ajax endpoint that allows an attacker to flood the log files with data at the maximum size allowed for a POST parameter per request. This can result in rapid consumption of disk space, potentially filling the entire disk. **CVE ID: CVE-2024-13925**		
Vendor: kofimokome					
Product: message_filter_for_contact_form_7					
Affected Version(s): * Up to (excluding) 1.6.3.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Apr-2025	7.6	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in kofimokome Message Filter for Contact Form 7 allows SQL Injection. This issue affects Message Filter for Contact Form 7: from n/a through 1.6.3.2. **CVE ID: CVE-2025-46252**	N/A	A-KOF-MESS-050525/55
Vendor: kovidgoyal					
Product: kitty					
Affected Version(s): * Up to (excluding) 0.41.0					
Origin Validation Error	20-Apr-2025	4.1	open_actions.py in kitty before 0.41.0 does not ask for user confirmation before running a local executable file that may have been linked from an untrusted document (e.g., a document opened in KDE ghostwriter). **CVE ID: CVE-2025-43929**	https://github.com/kovidgoyal/kitty/commit/ce5cfdd9caf44c538af800a07162e1f49bd53c35, https://github.com/kovidgoyal/kitty/compare/v0.40.1...v0.41.0	A-KOV-KITT-050525/56
Vendor: kuangstudy					
Product: kuangsimplebbs					
Affected Version(s): 1.0					
Improper	20-Apr-2025	6.3	A vulnerability was found in	N/A	A-KUA-KUAN-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			kuangstudy KuangSimpleBBS 1.0. It has been declared as critical. Affected by this vulnerability is the function fileUpload of the file src/main/java/com/kuang/controller/QuestionController.java. The manipulation of the argument editormd-image-file leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3830**		050525/57
Vendor: langgenius					
Product: dify					
Affected Version(s): * Up to (including) 0.6.8					
Improper Access Control	18-Apr-2025	6.5	Dify is an open-source LLM app development platform. Prior to version 0.6.12, a vulnerability was identified in the DIFY where normal users can enable or disable apps through the API, even though the web UI button for this action is disabled and normal users are not permitted to make such changes. This access control flaw allows non-admin users to make unauthorized changes, which can disrupt the functionality and availability of the APPS. This issue has been patched in version 0.6.12. A workaround for this vulnerability involves updating the API access control mechanisms to enforce stricter user role permissions and implementing role-based access controls (RBAC) to ensure that only users with admin privileges can send	https://github.com/langgenius/dify/pull/5266, https://github.com/langgenius/dify/security/advisories/GHSA-hqcx-598m-pjq4, https://github.com/langgenius/dify/security/advisories/GHSA-hqcx-598m-pjq4	A-LAN-DIFY-050525/58

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enable or disable requests for apps. **CVE ID: CVE-2025-32796**		
Vendor: litepublisher					
Product: litepubl_cms					
Affected Version(s): * Up to (including) 7.09					
Improper Control of Generation of Code ('Code Injection')	17-Apr-2025	7.2	Litepubl CMS <= 7.0.9 is vulnerable to RCE in admin/service/run. **CVE ID: CVE-2025-29661**	N/A	A-LIT-LITE-050525/59
Vendor: lm21					
Product: twonav					
Affected Version(s): 2.0.18-20241105					
Server-Side Request Forgery (SSRF)	17-Apr-2025	6.5	An issue in twonav v.2.1.18-20241105 allows a remote attacker to obtain sensitive information via the site settings component. **CVE ID: CVE-2025-29450**	N/A	A-LM2-TWON-050525/60
Affected Version(s): 2.1.18-20241105					
Server-Side Request Forgery (SSRF)	17-Apr-2025	6.5	An issue in twonav v.2.1.18-20241105 allows a remote attacker to obtain sensitive information via the link identification function. **CVE ID: CVE-2025-29449**	N/A	A-LM2-TWON-050525/61
Vendor: mayurik					
Product: online_student_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2025	6.1	A stored cross-site scripting (XSS) vulnerability fin Student Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the email parameter on the profile.php page.	N/A	A-MAY-ONLI-050525/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2023-44753		
Vendor: migaweb					
Product: simple_calendar_for_elementor					
Affected Version(s): * Up to (excluding) 1.6.5					
Cross-Site Request Forgery (CSRF)	22-Apr-2025	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Michael Simple calendar for Elementor allows Cross Site Request Forgery. This issue affects Simple calendar for Elementor: from n/a through 1.6.4. **CVE ID: CVE-2025-46249**	N/A	A-MIG-SIMP-050525/63
Vendor: mingsoft					
Product: mcms					
Affected Version(s): 5.4.3					
Unrestricted Upload of File with Dangerous Type	21-Apr-2025	9.8	An arbitrary file upload vulnerability in the ueditor component of MCMS v5.4.3 allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID: CVE-2025-29287**	N/A	A-MIN-MCMS-050525/64
Vendor: mirweiye					
Product: seven_bears_library_cms					
Affected Version(s): * Up to (excluding) 2023					
Server-Side Request Forgery (SSRF)	16-Apr-2025	2.7	A vulnerability was found in mirweiye Seven Bears Library CMS 2023. It has been classified as problematic. Affected is an unknown function of the component Add Link Handler. The manipulation leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3691**	N/A	A-MIR-SEVE-050525/65

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: multidots					
Product: advanced_linked_variations_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.0.4					
Missing Authorization	22-Apr-2025	5.3	Missing Authorization vulnerability in Dotstore Advanced Linked Variations for Woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Advanced Linked Variations for Woocommerce: from n/a through 1.0.3. **CVE ID: CVE-2025-46244**	N/A	A-MUL-ADVA-050525/66
Vendor: Mybb					
Product: mybb					
Affected Version(s): 1.8.38					
Server-Side Request Forgery (SSRF)	17-Apr-2025	7.6	An issue in MyBB 1.8.38 allows a remote attacker to obtain sensitive information via the Add Mycode function. NOTE: the Supplier disputes this because of the allowed actions of Board administrators and because of SSRF mitigation. **CVE ID: CVE-2025-29460**	N/A	A-MYB-MYBB-050525/67
Server-Side Request Forgery (SSRF)	17-Apr-2025	7.6	An issue in MyBB 1.8.38 allows a remote attacker to obtain sensitive information via the Change Avatar function. NOTE: the Supplier disputes this because of the allowed actions of Board administrators and because of SSRF mitigation. **CVE ID: CVE-2025-29458**	N/A	A-MYB-MYBB-050525/68
Server-Side Request Forgery (SSRF)	17-Apr-2025	7.6	An issue in MyBB 1.8.38 allows a remote attacker to obtain sensitive information via the Import a Theme function. NOTE: the	N/A	A-MYB-MYBB-050525/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supplier disputes this because of the allowed actions of Board administrators and because of SSRF mitigation. **CVE ID: CVE-2025-29457**		
Vendor: nodebb					
Product: nodebb					
Affected Version(s): * Up to (including) 4.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2025	6.1	Cross-Site Scripting (XSS) vulnerability in NodeBB v4.0.4 and before allows remote attackers to store arbitrary code and potentially render the blacklist IP functionality unusable until content is removed via the database. **CVE ID: CVE-2025-29512**	N/A	A-NOD-NODE-050525/70
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2025	6.1	Cross-Site Scripting (XSS) vulnerability in NodeBB v4.0.4 and before allows remote attackers to store arbitrary code in the admin API Access token generator. **CVE ID: CVE-2025-29513**	N/A	A-NOD-NODE-050525/71
Vendor: oceanwp					
Product: ocean_extra					
Affected Version(s): * Up to (excluding) 2.4.7					
Improper Control of Generation of Code ('Code Injection')	22-Apr-2025	6.5	The Ocean Extra plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.4.6. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes when WooCommerce is also	https://plugins.trac.wordpress.org/changeset/3277977/	A-OCE-OCEA-050525/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			installed and activated. **CVE ID: CVE-2025-3472**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2025	6.4	The Ocean Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'oceanwp_icon' shortcode in all versions up to, and including, 2.4.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2025-3457**	https://plugins.trac.wordpress.org/changeset/3277977/	A-OCE-OCEA-050525/73
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2025	6.4	The Ocean Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ocean_gallery_id' parameter in all versions up to, and including, 2.4.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The Classic Editor plugin must be installed and activated to exploit the vulnerability. **CVE ID: CVE-2025-3458**	https://plugins.trac.wordpress.org/changeset/3277977/	A-OCE-OCEA-050525/74
Vendor: omnissa					
Product: unified_access_gateway					
Affected Version(s): * Up to (excluding) 2503					
Permissive Cross-	17-Apr-2025	7.1	Omnissa UAG contains a Cross-Origin Resource	https://static.omnissa.com/site	A-OMN-UNIF-050525/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
domain Policy with Untrusted Domains			Sharing (CORS) bypass vulnerability. A malicious actor with network access to UAG may be able to bypass administrator-configured CORS restrictions to gain access to sensitive networks. **CVE ID: CVE-2025-25234**	s/default/files/OMSA-2025-0002.pdf, https://www.omnissa.com/omnissa-security-response/	
Vendor: open-metadata					
Product: openmetadata					
Affected Version(s): * Up to (including) 1.4.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Apr-2025	7.1	OpenMetadata <=1.4.1 is vulnerable to SQL Injection. An attacker can extract information from the database in function listCount in the WorkflowDAO interface. The workflowtype and status parameters can be used to build a SQL query. **CVE ID: CVE-2024-55238**	N/A	A-OPE-OPEN-050525/76
Vendor: oretnom23					
Product: online_eyewear_shop					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Apr-2025	2.4	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /oews/classes/Master.php?f=save_product. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3692**	N/A	A-ORE-ONLI-050525/77
Product: online_id_generator_system					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2025	9.8	Sourcecodester Online ID Generator System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at id_generator/admin/?page=generate/index&id=1. **CVE ID: CVE-2024-40072**	N/A	A-ORE-ONLI-050525/78
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2025	9.8	Sourcecodester Online ID Generator System 1.0 was discovered to contain a SQL injection vulnerability via the template parameter at id_generator/admin/?page=generate&template=4. **CVE ID: CVE-2024-40073**	N/A	A-ORE-ONLI-050525/79
Unrestricted Upload of File with Dangerous Type	16-Apr-2025	9.8	Sourcecodester Online ID Generator System 1.0 was discovered to contain an arbitrary file upload vulnerability via id_generator/classes/SystemSettings.php?f=update_settings. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID: CVE-2024-40071**	N/A	A-ORE-ONLI-050525/80
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2025	5.9	Sourcecodester Online ID Generator System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at id_generator/admin/?page=templates/manage_template&id=1. **CVE ID: CVE-2024-40068**	N/A	A-ORE-ONLI-050525/81
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Apr-2025	5.4	Sourcecodester Online ID Generator System 1.0 was discovered to contain Stored Cross Site Scripting (XSS) via id_generator/classes/Users.php?f=save, and the point of vulnerability is in the POST	N/A	A-ORE-ONLI-050525/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter 'firstname' and 'lastname'. **CVE ID: CVE-2024-40069**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Apr-2025	5.1	Sourcecodester Online ID Generator System 1.0 was discovered to contain an arbitrary file upload vulnerability via id_generator/classes/Users.php?f=save. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID: CVE-2024-40070**	N/A	A-ORE-ONLI-050525/83
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Apr-2025	4.8	Sourcecodester Online ID Generator System 1.0 was discovered to contain Stored Cross Site Scripting (XSS) via id_generator/classes/SystemSettings.php?f=update_settings, and the point of vulnerability is in the POST parameter 'short_name'. **CVE ID: CVE-2024-40074**	N/A	A-ORE-ONLI-050525/84
Product: student_study_center_desk_management_system					
Affected Version(s): 1.0					
Improper Authentication	22-Apr-2025	9.8	An issue in Student Study Center Desk Management System v1.0 allows attackers to bypass authentication via a crafted GET request to /php-sscdms/admin/login.php. **CVE ID: CVE-2023-44752**	N/A	A-ORE-STUD-050525/85
Vendor: Pbootcms					
Product: Pbootcms					
Affected Version(s): 3.2.5					
Server-Side Request Forgery (SSRF)	18-Apr-2025	2.7	A vulnerability was found in PbootCMS 3.2.5. It has been classified as problematic. Affected is an unknown function of the component	N/A	A-PBO-PBOO-050525/86

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Image Handler. The manipulation leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3787**		
Vendor: pcman					
Product: ftp_server					
Affected Version(s): 2.0.7					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Apr-2025	7.3	A vulnerability was found in PCMan FTP Server 2.0.7. It has been declared as critical. This vulnerability affects unknown code of the component SIZE Command Handler. The manipulation leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3683**	N/A	A-PCM-FTP_-050525/87
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Apr-2025	7.3	A vulnerability, which was classified as critical, was found in PCMan FTP Server 2.0.7. Affected is an unknown function of the component HOST Command Handler. The manipulation leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3679**	N/A	A-PCM-FTP_-050525/88
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Apr-2025	7.3	A vulnerability has been found in PCMan FTP Server 2.0.7 and classified as critical. Affected by this vulnerability is an unknown functionality of the component LANG Command Handler. The manipulation leads to buffer overflow.	N/A	A-PCM-FTP_-050525/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3680**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Apr-2025	7.3	A vulnerability was found in PCMan FTP Server 2.0.7 and classified as critical. Affected by this issue is some unknown functionality of the component MODE Command Handler. The manipulation leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3681**	N/A	A-PCM-FTP_-050525/90
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Apr-2025	7.3	A vulnerability was found in PCMan FTP Server 2.0.7. It has been classified as critical. This affects an unknown part of the component PASV Command Handler. The manipulation leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3682**	N/A	A-PCM-FTP_-050525/91
Vendor: personal-management-system					
Product: personal_management_system					
Affected Version(s): 1.4.65					
Server-Side Request Forgery (SSRF)	17-Apr-2025	6.5	An issue in personal-management-system Personal Management System 1.4.65 allows a remote attacker to obtain sensitive information via the Travel Ideas" function. **CVE ID: CVE-2025-29455**	N/A	A-PER-PERS-050525/92
Server-Side	17-Apr-2025	6.5	An issue in personal-	N/A	A-PER-PERS-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (SSRF)			management-system Personal Management System 1.4.65 allows a remote attacker to obtain sensitive information via the create Notes function. **CVE ID: CVE-2025-29456**		050525/93
Server-Side Request Forgery (SSRF)	17-Apr-2025	6.5	An issue in personal-management-system Personal Management System 1.4.65 allows a remote attacker to obtain sensitive information via the my-contacts-settings component. **CVE ID: CVE-2025-29453**	N/A	A-PER-PERS-050525/94
Server-Side Request Forgery (SSRF)	17-Apr-2025	6.5	An issue in personal-management-system Personal Management System 1.4.65 allows a remote attacker to obtain sensitive information via the Upload function. **CVE ID: CVE-2025-29454**	N/A	A-PER-PERS-050525/95
Vendor: phpgurukul					
Product: hostel_management_system					
Affected Version(s): 2.1					
Session Fixation	28-Apr-2025	9.1	A vulnerability was found in PHPGurukul Hostel Management System 2.1 in the /hostel/change-password.php file of the user panel - Change Password component. Improper handling of session data allows a Session Hijacking attack, exploitable remotely **CVE ID: CVE-2025-45953**	N/A	A-PHP-HOST-050525/96
Product: men_salon_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special	20-Apr-2025	7.3	A vulnerability was found in PHPGurukul Men Salon Management System 1.0. It	N/A	A-PHP-MEN_-050525/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			has been classified as critical. Affected is an unknown function of the file /admin/sales-reports-detail.php. The manipulation of the argument fromdate/todate leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3829**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Apr-2025	7.3	A vulnerability has been found in PHPGurukul Men Salon Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/forgot-password.php. The manipulation of the argument email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3827**	N/A	A-PHP-MEN_-050525/98
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Apr-2025	7.3	A vulnerability was found in PHPGurukul Men Salon Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/view-appointment.php?viewid=11. The manipulation of the argument remark leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well. **CVE ID: CVE-2025-3828**	N/A	A-PHP-MEN_-050525/99
Improper	16-Apr-2025	7.3	A vulnerability was found in	N/A	A-PHP-MEN_-

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')			PHPGurukul Men Salon Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/edit-services.php. The manipulation of the argument cost leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3690**		050525/100
Product: nipah_virus_testing_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	28-Apr-2025	7.3	A vulnerability, which was classified as critical, has been found in PHPGurukul Nipah Virus Testing Management System 1.0. This issue affects some unknown processing of the file /profile.php. The manipulation of the argument adminname leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-4026**	N/A	A-PHP-NIPA-050525/101
Product: old_age_home_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	28-Apr-2025	7.3	A vulnerability, which was classified as critical, was found in PHPGurukul Old Age Home Management System 1.0. Affected is an unknown function of the file /admin/rules.php. The manipulation of the argument pagetitle leads to sql injection. It is possible to launch the attack remotely. The exploit has been	N/A	A-PHP-OLD_-050525/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. **CVE ID: CVE-2025-4027**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	28-Apr-2025	7.3	A vulnerability was found in PHPGurukul Old Age Home Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /contact.php. The manipulation of the argument fname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well. **CVE ID: CVE-2025-4020**	N/A	A-PHP-OLD_-050525/103
Product: online_banquet_booking_system					
Affected Version(s): 1.2					
Improper Control of Generation of Code ('Code Injection')	28-Apr-2025	9.8	An issue in phpgurukul Online Banquet Booking System V1.2 allows an attacker to execute arbitrary code via the /obbs/change-password.php file of the My Account - Change Password component **CVE ID: CVE-2025-45947**	N/A	A-PHP-ONLI-050525/104
Product: pre-school_enrollment_system					
Affected Version(s): 1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Apr-2025	7.5	PHPGurukul Pre-School Enrollment System is vulnerable to Directory Traversal in manage-teachers.php. **CVE ID: CVE-2025-28072**	N/A	A-PHP-PRE--050525/105
Product: rail_pass_management_system					
Affected Version(s): 1.0					
Improper	28-Apr-2025	7.3	A vulnerability was found in	N/A	A-PHP-RAIL-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')			PHPGurukul Rail Pass Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/search-pass.php. The manipulation of the argument searchdata leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-4039**		050525/106
Product: user_registration_\&_login_and_user_management_system					
Affected Version(s): 3.3					
Session Fixation	28-Apr-2025	9.8	A critical vulnerability was found in PHPGurukul User Registration & Login and User Management System V3.3 in the /loginsystem/change-password.php file of the user panel - Change Password component. Improper handling of session data allows a Session Hijacking attack, exploitable remotely and leading to account takeover. **CVE ID: CVE-2025-45949**	N/A	A-PHP-USER-050525/107
Vendor: plechevandrey					
Product: wp-recall					
Affected Version(s): * Up to (excluding) 16.26.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Apr-2025	3.5	The WP-Recall WordPress plugin before 16.26.12 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	N/A	A-PLE-WP-R-050525/108

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-9771		
Vendor: plugin-planet					
Product: simple_download_counter					
Affected Version(s): * Up to (excluding) 2.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2025	6.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeff Starr Simple Download Counter allows Stored XSS. This issue affects Simple Download Counter: from n/a through 2.2. **CVE ID: CVE-2025-46240**	N/A	A-PLU-SIMP-050525/109
Product: theme_switcha					
Affected Version(s): * Up to (excluding) 3.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2025	6.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeff Starr Theme Switcha allows Stored XSS. This issue affects Theme Switcha: from n/a through 3.4. **CVE ID: CVE-2025-46239**	N/A	A-PLU-THEM-050525/110
Vendor: qualitia					
Product: active\!_mail					
Affected Version(s): * Up to (excluding) 6.60.05008562					
Stack-based Buffer Overflow	18-Apr-2025	9.8	Active! mail 6 BuildInfo: 6.60.05008561 and earlier contains a stack-based buffer overflow vulnerability. Receiving a specially crafted request created and sent by a remote unauthenticated attacker may lead to arbitrary code execution and/or a denial-of-service (DoS) condition. **CVE ID: CVE-2025-42599**	https://www.qualitia.com/jp/news/2025/04/18_1030.html	A-QUA-ACTI-050525/111

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: quasar					
Product: qmarkdown					
Affected Version(s): * Up to (excluding) 2.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-2025	4.9	QMarkdown (aka quasar-ui-qmarkdown) before 2.0.5 allows XSS via headers even when when no-html is set. **CVE ID: CVE-2025-43954**	https://github.com/quasarframework/quasar-ui-qmarkdown/commit/b61dff84851c45369cf931db5bd93db177c657f6, https://github.com/quasarframework/quasar-ui-qmarkdown/compare/v2.0.4...v2.0.5	A-QUA-QMAR-050525/112
Vendor: razormist					
Product: phone_management_system					
Affected Version(s): 1.0					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Apr-2025	5.3	A vulnerability classified as critical has been found in SourceCodester Phone Management System 1.0. This affects the function main of the component Password Handler. The manipulation of the argument s leads to buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3763**	N/A	A-RAZ-PHON-050525/113
Vendor: rolandbaer					
Product: list_last_changes					
Affected Version(s): * Up to (excluding) 1.2.2					
Improper Neutralization of Input During Web Page	22-Apr-2025	6.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rbaer List Last Changes	N/A	A-ROL-LIST-050525/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			allows Stored XSS. This issue affects List Last Changes: from n/a through 1.2.1. **CVE ID: CVE-2025-46238**		
Vendor: SAP					
Product: netweaver					
Affected Version(s): 7.50					
Unrestricted Upload of File with Dangerous Type	24-Apr-2025	10	SAP NetWeaver Visual Composer Metadata Uploader is not protected with a proper authorization, allowing unauthenticated agent to upload potentially malicious executable binaries that could severely harm the host system. This could significantly affect the confidentiality, integrity, and availability of the targeted system. **CVE ID: CVE-2025-31324**	https://url.sap/sapsecuritypatchday	A-SAP-NETW-050525/115
Vendor: senior-walter					
Product: web-based_pharmacy_product_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Apr-2025	7.3	A vulnerability, which was classified as critical, has been found in SourceCodester Web-based Pharmacy Product Management System 1.0. This issue affects some unknown processing of the file backup.php of the component Database Backup Handler. The manipulation of the argument txtdbname leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3729**	N/A	A-SEN-WEB--050525/116
Improper	20-Apr-2025	2.4	A vulnerability was found in	N/A	A-SEN-WEB--

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			SourceCodester Web-based Pharmacy Product Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file changepassword.php. The manipulation of the argument txtconfirm_password/txtnew_password/txtold_password leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3822**		050525/117
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-2025	2.4	A vulnerability was found in SourceCodester Web-based Pharmacy Product Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file add-admin.php. The manipulation of the argument txtpassword/txtfullname/txtemail leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3821**	N/A	A-SEN-WEB--050525/118
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-2025	2.4	A vulnerability, which was classified as problematic, was found in SourceCodester Web-based Pharmacy Product Management System 1.0. This affects an unknown part of the file add-supplier.php. The manipulation of the argument	N/A	A-SEN-WEB--050525/119

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			txtsupplier_name/txtaddress leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3826**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-2025	2.4	A vulnerability, which was classified as problematic, has been found in SourceCodester Web-based Pharmacy Product Management System 1.0. Affected by this issue is some unknown functionality of the file add-category.php. The manipulation of the argument txtcategory_name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3825**	N/A	A-SEN-WEB--050525/120
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-2025	2.4	A vulnerability classified as problematic was found in SourceCodester Web-based Pharmacy Product Management System 1.0. Affected by this vulnerability is an unknown functionality of the file add-product.php. The manipulation of the argument txtprice/txtproduct_name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3824**	N/A	A-SEN-WEB--050525/121
Improper Neutralization of Input During Web	20-Apr-2025	2.4	A vulnerability classified as problematic has been found in SourceCodester Web-based Pharmacy Product	N/A	A-SEN-WEB--050525/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			Management System 1.0. Affected is an unknown function of the file add-stock.php. The manipulation of the argument txttotalcost/txtproductID/txtprice/txtexpirydate leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3823**		
Vendor: seniorwalter					
Product: web-based_pharmacy_product_management_system					
Affected Version(s): 1.0					
Improper Access Control	18-Apr-2025	6.3	A vulnerability classified as critical was found in SourceCodester Web-based Pharmacy Product Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /add-product.php. The manipulation of the argument Avatar leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3783**	N/A	A-SEN-WEB--050525/123
Vendor: Seopanel					
Product: seo_panel					
Affected Version(s): 4.11.0					
Server-Side Request Forgery (SSRF)	17-Apr-2025	7.6	An issue in Seo Panel 4.11.0 allows a remote attacker to obtain sensitive information via the Proxy Manager component. **CVE ID: CVE-2025-29452**	N/A	A-SEO-SEO_-050525/124
Server-Side Request	17-Apr-2025	7.6	An issue in Seo Panel 4.11.0 allows a remote attacker to	N/A	A-SEO-SEO_-050525/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			obtain sensitive information via the Mail Setting component. **CVE ID: CVE-2025-29451**		
Vendor: servit					
Product: affiliate-toolkit					
Affected Version(s): * Up to (excluding) 3.7.4					
Cross-Site Request Forgery (CSRF)	22-Apr-2025	5.4	Cross-Site Request Forgery (CSRF) vulnerability in SERVIT Software Solutions affiliate-toolkit allows Cross Site Request Forgery. This issue affects affiliate-toolkit: from n/a through 3.7.3. **CVE ID: CVE-2025-46231**	N/A	A-SER-AFFI-050525/126
Vendor: sirv					
Product: sirv					
Affected Version(s): * Up to (excluding) 7.5.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2025	6.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sirv CDN and Image Hosting Sirv allows Stored XSS. This issue affects Sirv: from n/a through 7.5.3. **CVE ID: CVE-2025-46233**	N/A	A-SIR-SIRV-050525/127
Vendor: sktthemes					
Product: recover_abandoned_cart_for_woocommerce					
Affected Version(s): * Up to (excluding) 2.3					
Cross-Site Request Forgery (CSRF)	22-Apr-2025	4.3	Cross-Site Request Forgery (CSRF) vulnerability in sonalsinha21 Recover abandoned cart for WooCommerce allows Cross Site Request Forgery. This issue affects Recover abandoned cart for WooCommerce: from n/a through 2.2. **CVE ID: CVE-2025-46243**	N/A	A-SKT-RECO-050525/128

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: skt_blocks					
Affected Version(s): * Up to (excluding) 2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2025	6.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sonalsinha21 SKT Blocks – Gutenberg based Page Builder allows Stored XSS. This issue affects SKT Blocks – Gutenberg based Page Builder: from n/a through 2.0. **CVE ID: CVE-2025-46235**	N/A	A-SKT-SKT_-050525/129
Vendor: taxopress					
Product: taxopress					
Affected Version(s): * Up to (excluding) 3.30.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Apr-2025	3.5	The WordPress Tag, Category, and Taxonomy Manager WordPress plugin before 3.30.0 does not sanitise and escape some of its Widgets settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID: CVE-2025-0627**	N/A	A-TAX-TAXO-050525/130
Vendor: textmetrics					
Product: textmetrics					
Affected Version(s): * Up to (excluding) 3.6.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2025	5.9	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Israpil Textmetrics allows Stored XSS. This issue affects Textmetrics: from n/a through 3.6.2. **CVE ID: CVE-2025-46229**	N/A	A-TEX-TEXT-050525/131

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Thecartpress					
Product: boot_store					
Affected Version(s): 1.6.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Apr-2025	7.2	The TheCartPress boot-store (aka Boot Store) theme 1.6.4 for WordPress allows header.php tcp_register_error XSS. NOTE: CVE-2015-4582 is not assigned to any Oracle product. **CVE ID: CVE-2015-4582**	N/A	A-THE-BOOT-050525/132
Vendor: torrahclef					
Product: company_website_cms					
Affected Version(s): 1.0					
External Control of File Name or Path	16-Apr-2025	9.8	SourceCodester Company Website CMS 1.0 contains a file upload vulnerability via the "Create Services" file /dashboard/Services. **CVE ID: CVE-2025-29708**	N/A	A-TOR-COMP-050525/133
External Control of File Name or Path	16-Apr-2025	9.8	SourceCodester Company Website CMS 1.0 has a File upload vulnerability via the "Create portfolio" file /dashboard/portfolio. **CVE ID: CVE-2025-29709**	N/A	A-TOR-COMP-050525/134
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Apr-2025	6.1	SourceCodester Company Website CMS 1.0 is vulnerable to Cross Site Scripting (XSS) via /dashboard/Services. **CVE ID: CVE-2025-29710**	N/A	A-TOR-COMP-050525/135
Vendor: vikasratudi					
Product: lifetime_free_drag_\&_drop_contact_form_builder					
Affected Version(s): * Up to (excluding) 3.1.15					
Improper Neutralization of Input During Web Page	22-Apr-2025	5.9	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vikas Ratudi VForm allows	N/A	A-VIK-LIFE-050525/136

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Stored XSS. This issue affects VForm: from n/a through 3.1.14. **CVE ID: CVE-2025-46250**		
Vendor: visualcomposer					
Product: visual_composer_website_builder					
Affected Version(s): * Up to (excluding) 45.11.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2025	6.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Visual Composer Visual Composer Website Builder allows Stored XSS. This issue affects Visual Composer Website Builder: from n/a through 45.10.0. **CVE ID: CVE-2025-46254**	N/A	A-VIS-VISU-050525/137
Vendor: wpmet					
Product: gutenkit					
Affected Version(s): * Up to (excluding) 2.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2025	6.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ataur R GutenKit allows Stored XSS. This issue affects GutenKit: from n/a through 2.2.2. **CVE ID: CVE-2025-46253**	N/A	A-WPM-GUTE-050525/138
Vendor: xianqi					
Product: kindergarten_management_system					
Affected Version(s): 2.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Apr-2025	6.3	A vulnerability was found in Xianqi Kindergarten Management System 2.0 Bulid 20190808. It has been rated as critical. This issue affects some unknown processing of the file stu_list.php of the component Child Management. The	N/A	A-XIA-KIND-050525/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument sex leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well. **CVE ID: CVE-2025-3684**		
Vendor: Xmlsoft					
Product: libxml2					
Affected Version(s): * Up to (excluding) 2.13.8					
Improper Validation of Specified Quantity in Input	17-Apr-2025	2.9	In libxml2 before 2.13.8 and 2.14.x before 2.14.2, xmlSchemaIDCFillNodeTables in xmlschemas.c has a heap-based buffer under-read. To exploit this, a crafted XML document must be validated against an XML schema with certain identity constraints, or a crafted XML schema must be used. **CVE ID: CVE-2025-32415**	N/A	A-XML-LIBX-050525/140
Affected Version(s): From (including) 2.14.0 Up to (excluding) 2.14.2					
Improper Validation of Specified Quantity in Input	17-Apr-2025	2.9	In libxml2 before 2.13.8 and 2.14.x before 2.14.2, xmlSchemaIDCFillNodeTables in xmlschemas.c has a heap-based buffer under-read. To exploit this, a crafted XML document must be validated against an XML schema with certain identity constraints, or a crafted XML schema must be used. **CVE ID: CVE-2025-32415**	N/A	A-XML-LIBX-050525/141
Vendor: Xwiki					
Product: Xwiki					
Affected Version(s): From (including) 1.6 Up to (excluding) 15.10.16					
Improper Neutralizati	23-Apr-2025	8.8	XWiki is a generic wiki platform. In versions	https://github.com/xwiki/xwiki	A-XWI-XWIK-050525/142

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Special Elements used in an SQL Command ('SQL Injection')			starting from 1.6-milestone-1 to before 15.10.16, 16.4.6, and 16.10.1, it is possible for a user with SCRIPT right to escape from the HQL execution context and perform a blind SQL injection to execute arbitrary SQL statements on the database backend. Depending on the used database backend, the attacker may be able to not only obtain confidential information such as password hashes from the database, but also execute UPDATE/INSERT/DELETE queries. This issue has been patched in versions 16.10.1, 16.4.6 and 15.10.16. There is no known workaround, other than upgrading XWiki. The protection added to this REST API is the same as the one used to validate complete select queries, making it more consistent. However, while the script API always had this protection for complete queries, it's important to note that it's a very strict protection and some valid, but complex, queries might suddenly require the author to have programming right. **CVE ID: CVE-2025-32968**	- platform/security/advisories/GHSA-g9jj-75mx-wjcx, https://jira.xwiki.org/browse/XWIKI-22718	
Affected Version(s): From (including) 1.8 Up to (excluding) 15.10.16					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Apr-2025	9.8	XWiki is a generic wiki platform. In versions starting from 1.8 and prior to 15.10.16, 16.4.6, and 16.10.1, it is possible for a remote unauthenticated user to escape from the HQL execution context and perform a blind SQL injection to execute arbitrary SQL statements on	https://github.com/xwiki/xwiki-platform/commit/5c11a874bd24a581f534d283186e209bbccd8113, https://github.com/xwiki/xwiki-	A-XWI-XWIK-050525/143

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the database backend, including when "Prevent unregistered users from viewing pages, regardless of the page rights" and "Prevent unregistered users from editing pages, regardless of the page rights" options are enabled. Depending on the used database backend, the attacker may be able to not only obtain confidential information such as password hashes from the database, but also execute UPDATE/INSERT/DELETE queries. This issue has been patched in versions 16.10.1, 16.4.6 and 15.10.16. There is no known workaround, other than upgrading XWiki. **CVE ID: CVE-2025-32969**	platform/security/advisories/GHSA-f69v-xrj8-rhxf, https://jira.xwiki.org/browse/XWIKI-22691	
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.4.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Apr-2025	9.8	XWiki is a generic wiki platform. In versions starting from 1.8 and prior to 15.10.16, 16.4.6, and 16.10.1, it is possible for a remote unauthenticated user to escape from the HQL execution context and perform a blind SQL injection to execute arbitrary SQL statements on the database backend, including when "Prevent unregistered users from viewing pages, regardless of the page rights" and "Prevent unregistered users from editing pages, regardless of the page rights" options are enabled. Depending on the used database backend, the attacker may be able to not only obtain confidential information such as password hashes from the	https://github.com/xwiki/xwiki-platform/commit/5c11a874bd24a581f534d283186e209bbccd8113, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-f69v-xrj8-rhxf, https://jira.xwiki.org/browse/XWIKI-22691	A-XWI-XWIK-050525/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			database, but also execute UPDATE/INSERT/DELETE queries. This issue has been patched in versions 16.10.1, 16.4.6 and 15.10.16. There is no known workaround, other than upgrading XWiki. **CVE ID: CVE-2025-32969**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Apr-2025	8.8	XWiki is a generic wiki platform. In versions starting from 1.6-milestone-1 to before 15.10.16, 16.4.6, and 16.10.1, it is possible for a user with SCRIPT right to escape from the HQL execution context and perform a blind SQL injection to execute arbitrary SQL statements on the database backend. Depending on the used database backend, the attacker may be able to not only obtain confidential information such as password hashes from the database, but also execute UPDATE/INSERT/DELETE queries. This issue has been patched in versions 16.10.1, 16.4.6 and 15.10.16. There is no known workaround, other than upgrading XWiki. The protection added to this REST API is the same as the one used to validate complete select queries, making it more consistent. However, while the script API always had this protection for complete queries, it's important to note that it's a very strict protection and some valid, but complex, queries might suddenly require the author to have programming right. **CVE ID: CVE-2025-32968**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-g9jj-75mx-wjcx, https://jira.xwiki.org/browse/XWIKI-22718	A-XWI-XWIK-050525/145
Affected Version(s): From (including) 16.5.0 Up to (excluding) 16.10.1					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Apr-2025	9.8	XWiki is a generic wiki platform. In versions starting from 1.8 and prior to 15.10.16, 16.4.6, and 16.10.1, it is possible for a remote unauthenticated user to escape from the HQL execution context and perform a blind SQL injection to execute arbitrary SQL statements on the database backend, including when "Prevent unregistered users from viewing pages, regardless of the page rights" and "Prevent unregistered users from editing pages, regardless of the page rights" options are enabled. Depending on the used database backend, the attacker may be able to not only obtain confidential information such as password hashes from the database, but also execute UPDATE/INSERT/DELETE queries. This issue has been patched in versions 16.10.1, 16.4.6 and 15.10.16. There is no known workaround, other than upgrading XWiki. **CVE ID: CVE-2025-32969**	https://github.com/xwiki/xwiki-platform/commit/5c11a874bd24a581f534d283186e209bbccd8113, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-f69v-xrj8-rhxf, https://jira.xwiki.org/browse/XWIKI-22691	A-XWI-XWIK-050525/146
Affected Version(s): From (including) 16.5.0 Up to (including) 16.10.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Apr-2025	8.8	XWiki is a generic wiki platform. In versions starting from 1.6-milestone-1 to before 15.10.16, 16.4.6, and 16.10.1, it is possible for a user with SCRIPT right to escape from the HQL execution context and perform a blind SQL injection to execute arbitrary SQL statements on the database backend. Depending on the used database backend, the attacker may be able to not	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-g9jj-75mx-wjcx, https://jira.xwiki.org/browse/XWIKI-22718	A-XWI-XWIK-050525/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			only obtain confidential information such as password hashes from the database, but also execute UPDATE/INSERT/DELETE queries. This issue has been patched in versions 16.10.1, 16.4.6 and 15.10.16. There is no known workaround, other than upgrading XWiki. The protection added to this REST API is the same as the one used to validate complete select queries, making it more consistent. However, while the script API always had this protection for complete queries, it's important to note that it's a very strict protection and some valid, but complex, queries might suddenly require the author to have programming right. **CVE ID: CVE-2025-32968**		
Affected Version(s): From (including) 5.0 Up to (including) 16.7.1					
Exposure of Resource to Wrong Sphere	16-Apr-2025	4.7	XWiki Platform is a generic wiki platform. A vulnerability in versions from 5.0 to 16.7.1 affects users with Message Stream enabled and a wiki configured as closed from selecting "Prevent unregistered users to view pages" in the Administrations Rights. The vulnerability is that any message sent in a subwiki to "everyone" is actually sent to the farm: any visitor of the main wiki will be able to see that message through the Dashboard, even if the subwiki is configured to be private. This issue will not be patched as Message Stream has been deprecated in XWiki 16.8.0RC1 and is not maintained anymore. A	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-42fh-pvvh-999x, https://jira.xwiki.org/browse/XWIKI-17154, https://jira.xwiki.org/browse/XWIKI-17154	A-XWI-XWIK-050525/148

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workaround for this issue involves keeping Message Stream disabled by default. It's advised to keep it disabled from Administration > Social > Message Stream. **CVE ID: CVE-2025-32783**		
Vendor: xxyopen					
Product: novel-plus					
Affected Version(s): 3.5.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Apr-2025	6.3	A vulnerability classified as critical has been found in xxyopen Novel-Plus 3.5.0. This affects an unknown part of the file /api/front/search/books. The manipulation of the argument sort leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-3676**	N/A	A-XXY-NOVE-050525/149
Vendor: yassmittal					
Product: commercify					
Affected Version(s): 1.0					
Cross-Site Request Forgery (CSRF)	17-Apr-2025	6.3	A CSRF vulnerability in Commercify v1.0 allows remote attackers to perform unauthorized actions on behalf of authenticated users. The issue exists due to missing CSRF protection on sensitive endpoints. **CVE ID: CVE-2025-29722**	N/A	A-YAS-COMM-050525/150
Vendor: ylefebvre					
Product: link_library					
Affected Version(s): * Up to (excluding) 7.8.1					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2025	6.5	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Yannick Lefebvre Link Library allows Stored XSS. This issue affects Link Library: from n/a through 7.8. **CVE ID: CVE-2025-46237**	N/A	A-YLE-LINK-050525/151
Hardware					
Vendor: alfa					
Product: wifi_camppro					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Apr-2025	9.8	Buffer Overflow vulnerability in ALFA_CAMPRO-co-2.29 allows a remote attacker to execute arbitrary code via the newap_text_0 key value **CVE ID: CVE-2025-29045**	N/A	H-ALF-WIFI-050525/152
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Apr-2025	9.8	Buffer Overflow vulnerability inALFA WiFi CampPro router ALFA_CAMPRO-co-2.29 allows a remote attacker to execute arbitrary code via the GAPSMinute3 key value **CVE ID: CVE-2025-29046**	N/A	H-ALF-WIFI-050525/153
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Apr-2025	9.8	Buffer Overflow vulnerability inALFA WiFi CampPro router ALFA_CAMPRO-co-2.29 allows a remote attacker to execute arbitrary code via the hiddenIndex in the function StorageEditUser **CVE ID: CVE-2025-29047**	N/A	H-ALF-WIFI-050525/154
Vendor: Dlink					
Product: dir-816					
Affected Version(s): a2					
Improper Neutralizati	22-Apr-2025	6.5	D-Link DIR-816 A2V1.1.0B05 was found to	N/A	H-DLI-DIR--050525/155

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Special Elements used in a Command ('Command Injection')			contain a command injection in /goform/delRouting. **CVE ID: CVE-2025-29743**		
Product: dir-823x					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Apr-2025	9.8	An issue in dlink DIR 823x 240802 allows a remote attacker to execute arbitrary code via the target_addr key value and the function 0x41737c **CVE ID: CVE-2025-29040**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--050525/156
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Apr-2025	9.8	An issue in dlink DIR 832x 240802 allows a remote attacker to execute arbitrary code via the macaddr key value to the function 0x42232c **CVE ID: CVE-2025-29042**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--050525/157
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Apr-2025	9.8	An issue in dlink DIR 823x 240802 allows a remote attacker to execute arbitrary code via the target_addr key value and the function 0x41710c **CVE ID: CVE-2025-29041**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--050525/158
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Apr-2025	9.8	An issue in dlink DIR 832x 240802 allows a remote attacker to execute arbitrary code via the function 0x417234 **CVE ID: CVE-2025-29043**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--050525/159
Improper Control of	17-Apr-2025	7.2	An issue in dlink DIR 832x 240802 allows a remote	N/A	H-DLI-DIR--050525/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			attacker to execute arbitrary code via the function 0x41dda8 **CVE ID: CVE-2025-29039**		
Vendor: infodraw					
Product: pmrs-102					
Affected Version(s): -					
Path Traversal: '../filedir'	20-Apr-2025	5.8	In Infodraw Media Relay Service (MRS) 7.1.0.0, the MRS web server (on port 12654) allows reading arbitrary files via ../ directory traversal in the username field. Reading ServerParameters.xml may reveal administrator credentials in cleartext or with MD5 hashing. **CVE ID: CVE-2025-43928**	N/A	H-INF-PMRS-050525/161
Vendor: Netgear					
Product: r6100					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Apr-2025	9.8	Buffer Overflow vulnerability in Netgear-R61 router V1.0.1.28 allows a remote attacker to execute arbitrary code via the QUERY_STRING key value **CVE ID: CVE-2025-29044**	N/A	H-NET-R610-050525/162
Vendor: Tenda					
Product: ac10					
Affected Version(s): 4.0					
Stack-based Buffer Overflow	17-Apr-2025	7.5	Tenda AC10 V4.0si_V16.03.10.20 is vulnerable to Buffer Overflow in AdvSetMacMtuWan via wanMTU2. **CVE ID: CVE-2025-25455**	N/A	H-TEN-AC10-050525/163
Stack-based Buffer	17-Apr-2025	7.5	Tenda AC10 V4.0si_V16.03.10.20 is	N/A	H-TEN-AC10-050525/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow			vulnerable to Buffer Overflow in AdvSetMacMtuWan via cloneType2. **CVE ID: CVE-2025-25457**		
Stack-based Buffer Overflow	17-Apr-2025	7.5	Tenda AC10 V4.0si_V16.03.10.20 is vulnerable to Buffer Overflow in AdvSetMacMtuWan via wanSpeed2. **CVE ID: CVE-2025-25454**	N/A	H-TEN-AC10-050525/165
Product: ac15					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Apr-2025	8.8	A vulnerability was found in Tenda AC15 up to 15.03.05.19 and classified as critical. This issue affects the function fromSetWirelessRepeat of the file /goform/WifiExtraSet. The manipulation of the argument mac leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3786**	N/A	H-TEN-AC15-050525/166
Product: ac9					
Affected Version(s): 1.0					
Stack-based Buffer Overflow	23-Apr-2025	9.8	In the Tenda ac9 v1.0 router with firmware V15.03.05.14_multi, there is a stack overflow vulnerability in /goform/WifiWpsStart, which may lead to remote arbitrary code execution. **CVE ID: CVE-2025-45429**	N/A	H-TEN-AC9-050525/167
Stack-based Buffer Overflow	23-Apr-2025	9.8	In Tenda ac9 v1.0 with firmware V15.03.05.14_multi, the rebootTime parameter of	N/A	H-TEN-AC9-050525/168

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/goform/SetSysAutoRebbotCfg has a stack overflow vulnerability, which can lead to remote arbitrary code execution. **CVE ID: CVE-2025-45428**		
Stack-based Buffer Overflow	23-Apr-2025	9.8	In Tenda AC9 v1.0 with firmware V15.03.05.14_multi, the security parameter of /goform/WifiBasicSet has a stack overflow vulnerability, which can lead to remote arbitrary code execution. **CVE ID: CVE-2025-45427**	N/A	H-TEN-AC9-050525/169
Vendor: think					
Product: tk-rt-wr135g					
Affected Version(s): -					
Reliance on Cookies without Validation and Integrity Checking	17-Apr-2025	8.4	An issue in Think Router Tk-Rt-Wr135G V3.0.2-X000 allows attackers to bypass authentication via a crafted cookie. **CVE ID: CVE-2024-55211**	N/A	H-THI-TK-R-050525/170
Vendor: totolink					
Product: a3000ru					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A950RG V4.1.2cu.5161_B20200903 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28036**	N/A	H-TOT-A300-050525/171
Improper Neutralization of Special Elements used in an OS	22-Apr-2025	9.8	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102,	N/A	H-TOT-A300-050525/172

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth remote command execution vulnerability in the NTPSyncWithHost function through the hostTime parameter. **CVE ID: CVE-2025-28034**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A830R V4.1.2cu.5182_B20201102 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28035**	N/A	H-TOT-A300-050525/173
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpForm parameter. **CVE ID: CVE-2025-28032**	N/A	H-TOT-A300-050525/174
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903,	N/A	H-TOT-A300-050525/175

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpTo parameter. **CVE ID: CVE-2025-28033**		
Product: a3100r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth remote command execution vulnerability in the NTPSyncWithHost function through the hostTime parameter. **CVE ID: CVE-2025-28034**	N/A	H-TOT-A310-050525/176
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A950RG V4.1.2cu.5161_B20200903 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28036**	N/A	H-TOT-A310-050525/177
Improper Neutralization of Special Elements used in an OS	22-Apr-2025	9.8	TOTOLINK A830R V4.1.2cu.5182_B20201102 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function	N/A	H-TOT-A310-050525/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			through the NoticeUrl parameter. **CVE ID: CVE-2025-28035**		
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpForm parameter. **CVE ID: CVE-2025-28032**	N/A	H-TOT-A310-050525/179
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpTo parameter. **CVE ID: CVE-2025-28033**	N/A	H-TOT-A310-050525/180
Product: a3700r					
Affected Version(s): -					
Incorrect Privilege Assignment	16-Apr-2025	5.3	A vulnerability was found in TOTOLINK A3700R 9.1.2u.5822_B20200513. It has been declared as critical. Affected by this	N/A	H-TOT-A370-050525/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is the function setUrlFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3674**		
Product: a800r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A830R V4.1.2cu.5182_B20201102 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28035**	N/A	H-TOT-A800-050525/182
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A950RG V4.1.2cu.5161_B20200903 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28036**	N/A	H-TOT-A800-050525/183
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth remote command execution vulnerability in the NTPSyncWithHost function through the	N/A	H-TOT-A800-050525/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hostTime parameter. **CVE ID: CVE-2025-28034**		
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpTo parameter. **CVE ID: CVE-2025-28033**	N/A	H-TOT-A800-050525/185
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpForm parameter. **CVE ID: CVE-2025-28032**	N/A	H-TOT-A800-050525/186
Product: a810r					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	22-Apr-2025	9.8	TOTOLINK A810R V4.1.2cu.5182_B20201026 was found to contain a buffer overflow vulnerability in the cstecgi.cgi	N/A	H-TOT-A810-050525/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')			**CVE ID: CVE-2025-28024**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A950RG V4.1.2cu.5161_B20200903 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28036**	N/A	H-TOT-A810-050525/188
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth remote command execution vulnerability in the NTPSyncWithHost function through the hostTime parameter. **CVE ID: CVE-2025-28034**	N/A	H-TOT-A810-050525/189
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A830R V4.1.2cu.5182_B20201102 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28035**	N/A	H-TOT-A810-050525/190
Improper Neutralization of Special Elements used in an OS Command ('OS Command	22-Apr-2025	9.8	TOTOLINK A810R V4.1.2cu.5182_B20201026 and A950RG V4.1.2cu.5161_B20200903 were found to contain a pre-auth remote command execution vulnerability in the setDiagnosisCfg function through the	N/A	H-TOT-A810-050525/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Injection')			ipDomain parameter. **CVE ID: CVE-2025-28037**		
Stack-based Buffer Overflow	22-Apr-2025	8.8	TOTOLINK A810R V4.1.2cu.5182_B20201026 was discovered to contain a stack overflow via the startTime and endTime parameters in setParentalRules function. **CVE ID: CVE-2025-28030**	N/A	H-TOT-A810-050525/192
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpTo parameter. **CVE ID: CVE-2025-28033**	N/A	H-TOT-A810-050525/193
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpForm parameter. **CVE ID: CVE-2025-28032**	N/A	H-TOT-A810-050525/194

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: a830r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A830R V4.1.2cu.5182_B20201102 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28035**	N/A	H-TOT-A830-050525/195
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth remote command execution vulnerability in the NTPSyncWithHost function through the hostTime parameter. **CVE ID: CVE-2025-28034**	N/A	H-TOT-A830-050525/196
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A950RG V4.1.2cu.5161_B20200903 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28036**	N/A	H-TOT-A830-050525/197
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903,	N/A	H-TOT-A830-050525/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpForm parameter. **CVE ID: CVE-2025-28032**		
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpTo parameter. **CVE ID: CVE-2025-28033**	N/A	H-TOT-A830-050525/199
Product: a950rg					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A810R V4.1.2cu.5182_B20201026 and A950RG V4.1.2cu.5161_B20200903 were found to contain a pre-auth remote command execution vulnerability in the setDiagnosisCfg function through the ipDomain parameter. **CVE ID: CVE-2025-28037**	N/A	H-TOT-A950-050525/200
Improper Neutralization of Special Elements used in an	22-Apr-2025	9.8	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R	N/A	H-TOT-A950-050525/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth remote command execution vulnerability in the NTPSyncWithHost function through the hostTime parameter. **CVE ID: CVE-2025-28034**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A830R V4.1.2cu.5182_B20201102 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28035**	N/A	H-TOT-A950-050525/202
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A950RG V4.1.2cu.5161_B20200903 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28036**	N/A	H-TOT-A950-050525/203
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function	N/A	H-TOT-A950-050525/204

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through the IpTo parameter. **CVE ID: CVE-2025-28033**		
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpForm parameter. **CVE ID: CVE-2025-28032**	N/A	H-TOT-A950-050525/205
Product: ex1200t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK EX1200T V4.1.2cu.5232_B20210713 was found to contain a pre-auth remote command execution vulnerability in the setWebWlanIdx function through the webWlanIdx parameter. **CVE ID: CVE-2025-28038**	N/A	H-TOT-EX12-050525/206
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK EX1200T V4.1.2cu.5232_B20210713 was found to contain a pre-auth remote command execution vulnerability in the setUpgradeFW function through the FileName parameter. **CVE ID: CVE-2025-28039**	N/A	H-TOT-EX12-050525/207
Product: x18					
Affected Version(s): -					
Improper Neutralizati	18-Apr-2025	9.8	TOTOLINK X18 v9.1.0cu.2024_B20220329	N/A	H-TOT-X18-050525/208

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Special Elements used in a Command ('Command Injection')			has an unauthorized arbitrary command execution in the enable parameter' of the sub_41105C function of cstecgi .cgi. **CVE ID: CVE-2025-29209**		
Vendor: Tp-link					
Product: eap120					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2025	7.3	SQL Injection vulnerability exists in the TP-Link EAP120 router s login dashboard (version 1.0), allowing an unauthenticated attacker to inject malicious SQL statements via the login fields. NOTE: this is disputed because the issue can only be reproduced on a supplier-provided emulator, where access control is intentionally absent for ease of functional testing. **CVE ID: CVE-2025-29648**	N/A	H-TP--EAP1-050525/209
Product: m7000					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2025	9.8	SQL Injection vulnerability exists in the TP-Link M7000 4G LTE Mobile Wi-Fi Router Firmware Version: 1.0.7 Build 180127 Rel.55998n, allowing an unauthenticated attacker to inject malicious SQL statements via the username and password fields. NOTE: this is disputed because the issue can only be reproduced on a supplier-provided emulator, where access control is intentionally absent for ease of functional testing.	N/A	H-TP--M700-050525/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-29652		
Product: m7200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2025	6.3	SQL Injection vulnerability exists in the TP-Link M7200 4G LTE Mobile Wi-Fi Router Firmware Version: 1.0.7 Build 180127 Rel.55998n, allowing an unauthenticated attacker to inject malicious SQL statements via the username and password fields. NOTE: this is disputed because the issue can only be reproduced on a supplier-provided emulator, where access control is intentionally absent for ease of functional testing. **CVE ID: CVE-2025-29650**	N/A	H-TP--M720-050525/211
Product: m7450					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2025	9.8	SQL Injection vulnerability exists in the TP-Link M7450 4G LTE Mobile Wi-Fi Router Firmware Version: 1.0.2 Build 170306 Rel.1015n, allowing an unauthenticated attacker to inject malicious SQL statements via the username and password fields. **CVE ID: CVE-2025-29653**	N/A	H-TP--M745-050525/212
Product: m7650					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	16-Apr-2025	9.8	SQL Injection vulnerability exists in the TP-Link M7650 4G LTE Mobile Wi-Fi Router Firmware Version: 1.0.7 Build 170623 Rel.1022n, allowing an unauthenticated attacker to inject malicious SQL	N/A	H-TP--M765-050525/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Injection')			statements via the username and password fields. NOTE: this is disputed because the issue can only be reproduced on a supplier-provided emulator, where access control is intentionally absent for ease of functional testing. **CVE ID: CVE-2025-29651**		
Product: tl-wr840n					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2025	7.3	SQL Injection vulnerability exists in the TP-Link TL-WR840N router s login dashboard (version 1.0), allowing an unauthenticated attacker to inject malicious SQL statements via the username and password fields. NOTE: this is disputed because the issue can only be reproduced on a supplier-provided emulator, where access control is intentionally absent for ease of functional testing. **CVE ID: CVE-2025-29649**	N/A	H-TP--TL-W-050525/214
Operating System					
Vendor: alfa					
Product: wifi_camppro_firmware					
Affected Version(s): 2.29					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Apr-2025	9.8	Buffer Overflow vulnerability in ALFA_CAMPRO-co-2.29 allows a remote attacker to execute arbitrary code via the newap_text_0 key value **CVE ID: CVE-2025-29045**	N/A	O-ALF-WIFI-050525/215
Buffer Copy without Checking Size of Input ('Classic	17-Apr-2025	9.8	Buffer Overflow vulnerability inALFA WiFi CampPro router ALFA_CAMPRO-co-2.29 allows a remote attacker to	N/A	O-ALF-WIFI-050525/216

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			execute arbitrary code via the GAPSMinute3 key value **CVE ID: CVE-2025-29046**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Apr-2025	9.8	Buffer Overflow vulnerability inALFA WiFi CampPro router ALFA_CAMPRO-co-2.29 allows a remote attacker to execute arbitrary code via the hiddenIndex in the function StorageEditUser **CVE ID: CVE-2025-29047**	N/A	O-ALF-WIFI-050525/217
Vendor: Apple					
Product: ipados					
Affected Version(s): * Up to (excluding) 17.7.6					
Use After Free	29-Apr-2025	9.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to corrupt process memory. **CVE ID: CVE-2025-24252**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-IPAD-050525/218
Incorrect Authorization	29-Apr-2025	7.7	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to bypass authentication policy.	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-	O-APP-IPAD-050525/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-24206	us/122375, https://support.apple.com/en-us/122377	
NULL Pointer Dereference	29-Apr-2025	6.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, watchOS 11.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-24251**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122376	O-APP-IPAD-050525/220
Exposure of Sensitive Information to an Unauthorized Actor	29-Apr-2025	5.7	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to leak sensitive user information. **CVE ID: CVE-2025-24270**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-IPAD-050525/221
NULL Pointer Dereference	29-Apr-2025	5.7	A null pointer dereference was addressed with improved input validation. This issue is fixed in iOS 18.3 and iPadOS 18.3, visionOS 2.3, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, macOS Sequoia 15.3, tvOS 18.3. An attacker on the local network may be able to cause a denial-of-	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073,	O-APP-IPAD-050525/222

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service. **CVE ID: CVE-2025-24179**	https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122374	
Use After Free	29-Apr-2025	5.7	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-31197**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-IPAD-050525/223
Missing Authentication for Critical Function	29-Apr-2025	5.4	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An unauthenticated user on the same network as a signed-in Mac could send it AirPlay commands without pairing. **CVE ID: CVE-2025-24271**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-IPAD-050525/224
Affected Version(s): * Up to (excluding) 18.4.1					
Out-of-bounds Write	16-Apr-2025	7.5	A memory corruption issue was addressed with improved bounds checking. This issue is fixed in tvOS 18.4.1, visionOS 2.4.1, iOS iOS 18.4.1 and iPadOS 18.4.1, macOS Sequoia 15.4.1. Processing an audio	https://support.apple.com/en-us/122282, https://support.apple.com/en-us/122400, https://support.apple.com/en-	O-APP-IPAD-050525/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stream in a maliciously crafted media file may result in code execution. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on iOS. **CVE ID: CVE-2025-31200**	us/122401, https://support.apple.com/en-us/122402	
N/A	16-Apr-2025	6.8	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 18.4.1, visionOS 2.4.1, iOS iOS 18.4.1 and iPadOS 18.4.1, macOS Sequoia 15.4.1. An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on iOS. **CVE ID: CVE-2025-31201**	https://support.apple.com/en-us/122282, https://support.apple.com/en-us/122400, https://support.apple.com/en-us/122401, https://support.apple.com/en-us/122402	O-APP-IPAD-050525/226
Affected Version(s): From (including) 18.0 Up to (excluding) 18.3					
NULL Pointer Dereference	29-Apr-2025	5.7	A null pointer dereference was addressed with improved input validation. This issue is fixed in iOS 18.3 and iPadOS 18.3, visionOS 2.3, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, macOS Sequoia 15.3, tvOS 18.3. An attacker on the local network may be able to cause a denial-of-service. **CVE ID: CVE-2025-24179**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122374	O-APP-IPAD-050525/227
Affected Version(s): From (including) 18.0 Up to (excluding) 18.4					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	29-Apr-2025	9.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to corrupt process memory. **CVE ID: CVE-2025-24252**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-IPAD-050525/228
Incorrect Authorization	29-Apr-2025	7.7	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to bypass authentication policy. **CVE ID: CVE-2025-24206**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-IPAD-050525/229
NULL Pointer Dereference	29-Apr-2025	6.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, watchOS 11.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-24251**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.	O-APP-IPAD-050525/230

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.com/en-us/122376	
Exposure of Sensitive Information to an Unauthorized Actor	29-Apr-2025	5.7	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to leak sensitive user information. **CVE ID: CVE-2025-24270**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-IPAD-050525/231
Use After Free	29-Apr-2025	5.7	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-31197**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-IPAD-050525/232
Missing Authentication for Critical Function	29-Apr-2025	5.4	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An unauthenticated user on the same network as a signed-in Mac could send it AirPlay commands without pairing.	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-	O-APP-IPAD-050525/233

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-24271	us/122375, https://support.apple.com/en-us/122377	
Product: iphone_os					
Affected Version(s): * Up to (excluding) 18.3					
NULL Pointer Dereference	29-Apr-2025	5.7	A null pointer dereference was addressed with improved input validation. This issue is fixed in iOS 18.3 and iPadOS 18.3, visionOS 2.3, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, macOS Sequoia 15.3, tvOS 18.3. An attacker on the local network may be able to cause a denial-of-service. **CVE ID: CVE-2025-24179**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122374	O-APP-IPHO-050525/234
Affected Version(s): * Up to (excluding) 18.4					
Use After Free	29-Apr-2025	9.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to corrupt process memory. **CVE ID: CVE-2025-24252**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-IPHO-050525/235
Incorrect Authorization	29-Apr-2025	7.7	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.	O-APP-IPHO-050525/236

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to bypass authentication policy. **CVE ID: CVE-2025-24206**	apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	
NULL Pointer Dereference	29-Apr-2025	6.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, watchOS 11.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-24251**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122376	O-APP-IPHO-050525/237
Exposure of Sensitive Information to an Unauthorized Actor	29-Apr-2025	5.7	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to leak sensitive user information. **CVE ID: CVE-2025-24270**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-IPHO-050525/238
Use After Free	29-Apr-2025	5.7	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5,	https://support.apple.com/en-us/122371, https://support.apple.com/en-	O-APP-IPHO-050525/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-31197**	us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	
Missing Authentication for Critical Function	29-Apr-2025	5.4	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An unauthenticated user on the same network as a signed-in Mac could send it AirPlay commands without pairing. **CVE ID: CVE-2025-24271**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-IPHO-050525/240
Affected Version(s): * Up to (excluding) 18.4.1					
Out-of-bounds Write	16-Apr-2025	7.5	A memory corruption issue was addressed with improved bounds checking. This issue is fixed in tvOS 18.4.1, visionOS 2.4.1, iOS iOS 18.4.1 and iPadOS 18.4.1, macOS Sequoia 15.4.1. Processing an audio stream in a maliciously crafted media file may result in code execution. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on iOS. **CVE ID: CVE-2025-31200**	https://support.apple.com/en-us/122282, https://support.apple.com/en-us/122400, https://support.apple.com/en-us/122401, https://support.apple.com/en-us/122402	O-APP-IPHO-050525/241

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Apr-2025	6.8	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 18.4.1, visionOS 2.4.1, iOS iOS 18.4.1 and iPadOS 18.4.1, macOS Sequoia 15.4.1. An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on iOS. **CVE ID: CVE-2025-31201**	https://support.apple.com/en-us/122282, https://support.apple.com/en-us/122400, https://support.apple.com/en-us/122401, https://support.apple.com/en-us/122402	O-APP-IPHO-050525/242
Product: macos					
Affected Version(s): * Up to (excluding) 13.7.5					
Use After Free	29-Apr-2025	9.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to corrupt process memory. **CVE ID: CVE-2025-24252**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-MACO-050525/243
Incorrect Authorization	29-Apr-2025	7.7	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-	O-APP-MACO-050525/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass authentication policy. **CVE ID: CVE-2025-24206**	us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	
NULL Pointer Dereference	29-Apr-2025	6.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, watchOS 11.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-24251**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122376	O-APP-MACO-050525/245
Exposure of Sensitive Information to an Unauthorized Actor	29-Apr-2025	5.7	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to leak sensitive user information. **CVE ID: CVE-2025-24270**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-MACO-050525/246
NULL Pointer Dereference	29-Apr-2025	5.7	A null pointer dereference was addressed with improved input validation. This issue is fixed in iOS 18.3 and iPadOS 18.3, visionOS 2.3, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, macOS Sequoia 15.3,	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122072,	O-APP-MACO-050525/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tvOS 18.3. An attacker on the local network may be able to cause a denial-of-service. **CVE ID: CVE-2025-24179**	https://support.apple.com/en-us/122073, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122374	
Use After Free	29-Apr-2025	5.7	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-31197**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-MACO-050525/248
Missing Authentication for Critical Function	29-Apr-2025	5.4	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An unauthenticated user on the same network as a signed-in Mac could send it AirPlay commands without pairing. **CVE ID: CVE-2025-24271**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-MACO-050525/249
Affected Version(s): * Up to (excluding) 15.4.1					
Out-of-bounds Write	16-Apr-2025	7.5	A memory corruption issue was addressed with improved bounds checking. This issue is fixed in tvOS 18.4.1, visionOS 2.4.1, iOS	https://support.apple.com/en-us/122282, https://support.apple.com/en-	O-APP-MACO-050525/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iOS 18.4.1 and iPadOS 18.4.1, macOS Sequoia 15.4.1. Processing an audio stream in a maliciously crafted media file may result in code execution. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on iOS. **CVE ID: CVE-2025-31200**	us/122400, https://support.apple.com/en-us/122401, https://support.apple.com/en-us/122402	
N/A	16-Apr-2025	6.8	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 18.4.1, visionOS 2.4.1, iOS iOS 18.4.1 and iPadOS 18.4.1, macOS Sequoia 15.4.1. An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on iOS. **CVE ID: CVE-2025-31201**	https://support.apple.com/en-us/122282, https://support.apple.com/en-us/122400, https://support.apple.com/en-us/122401, https://support.apple.com/en-us/122402	O-APP-MACO-050525/251
Affected Version(s): From (including) 14.0 Up to (excluding) 14.7.5					
Use After Free	29-Apr-2025	9.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to corrupt process memory. **CVE ID: CVE-2025-24252**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-	O-APP-MACO-050525/252

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/122377	
Incorrect Authorization	29-Apr-2025	7.7	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to bypass authentication policy. **CVE ID: CVE-2025-24206**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-MACO-050525/253
NULL Pointer Dereference	29-Apr-2025	6.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, watchOS 11.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-24251**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122376	O-APP-MACO-050525/254
NULL Pointer Dereference	29-Apr-2025	5.7	A null pointer dereference was addressed with improved input validation. This issue is fixed in iOS 18.3 and iPadOS 18.3, visionOS 2.3, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, macOS Sequoia 15.3, tvOS 18.3. An attacker on the local network may be able to cause a denial-of-service.	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073, https://support.apple.com/en-us/122372,	O-APP-MACO-050525/255

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-24179	https://support.apple.com/en-us/122374	
Exposure of Sensitive Information to an Unauthorized Actor	29-Apr-2025	5.7	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to leak sensitive user information. **CVE ID: CVE-2025-24270**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-MACO-050525/256
Use After Free	29-Apr-2025	5.7	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-31197**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-MACO-050525/257
Missing Authentication for Critical Function	29-Apr-2025	5.4	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An unauthenticated user on the same network as a signed-in Mac could send it AirPlay commands without	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.	O-APP-MACO-050525/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pairing. **CVE ID: CVE-2025-24271**	apple.com/en-us/122375, https://support.apple.com/en-us/122377	
Affected Version(s): From (including) 15.0 Up to (excluding) 15.3					
NULL Pointer Dereference	29-Apr-2025	5.7	A null pointer dereference was addressed with improved input validation. This issue is fixed in iOS 18.3 and iPadOS 18.3, visionOS 2.3, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, macOS Sequoia 15.3, tvOS 18.3. An attacker on the local network may be able to cause a denial-of-service. **CVE ID: CVE-2025-24179**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122374	O-APP-MACO-050525/259
Affected Version(s): From (including) 15.0 Up to (excluding) 15.4					
Use After Free	29-Apr-2025	9.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to corrupt process memory. **CVE ID: CVE-2025-24252**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-MACO-050525/260
Incorrect Authorization	29-Apr-2025	7.7	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.	O-APP-MACO-050525/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to bypass authentication policy. **CVE ID: CVE-2025-24206**	apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	
NULL Pointer Dereference	29-Apr-2025	6.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, watchOS 11.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-24251**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122376	O-APP-MACO-050525/262
Exposure of Sensitive Information to an Unauthorized Actor	29-Apr-2025	5.7	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to leak sensitive user information. **CVE ID: CVE-2025-24270**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-MACO-050525/263
Use After Free	29-Apr-2025	5.7	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5,	https://support.apple.com/en-us/122371, https://support.apple.com/en-	O-APP-MACO-050525/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-31197**	us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	
Missing Authentication for Critical Function	29-Apr-2025	5.4	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An unauthenticated user on the same network as a signed-in Mac could send it AirPlay commands without pairing. **CVE ID: CVE-2025-24271**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-MACO-050525/265
Product: tvos					
Affected Version(s): * Up to (excluding) 18.3					
NULL Pointer Dereference	29-Apr-2025	5.7	A null pointer dereference was addressed with improved input validation. This issue is fixed in iOS 18.3 and iPadOS 18.3, visionOS 2.3, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, macOS Sequoia 15.3, tvOS 18.3. An attacker on the local network may be able to cause a denial-of-service. **CVE ID: CVE-2025-24179**	https://support.apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073, https://support.apple.com/en-us/122372, https://support.apple.com/en-	O-APP-TVOS-050525/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/122374	
Affected Version(s): * Up to (excluding) 18.4					
Use After Free	29-Apr-2025	9.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to corrupt process memory. **CVE ID: CVE-2025-24252**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-TVOS-050525/267
Incorrect Authorization	29-Apr-2025	7.7	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to bypass authentication policy. **CVE ID: CVE-2025-24206**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-TVOS-050525/268
NULL Pointer Dereference	29-Apr-2025	6.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, watchOS 11.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination.	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.	O-APP-TVOS-050525/269

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-24251	apple.com/en-us/122375, https://support.apple.com/en-us/122376	
Exposure of Sensitive Information to an Unauthorized Actor	29-Apr-2025	5.7	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to leak sensitive user information. **CVE ID: CVE-2025-24270**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-TVOS-050525/270
Use After Free	29-Apr-2025	5.7	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-31197**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-TVOS-050525/271
Missing Authentication for Critical Function	29-Apr-2025	5.4	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An unauthenticated user on the same network as a	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-	O-APP-TVOS-050525/272

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			signed-in Mac could send it AirPlay commands without pairing. **CVE ID: CVE-2025-24271**	us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	
Affected Version(s): * Up to (excluding) 18.4.1					
Out-of-bounds Write	16-Apr-2025	7.5	A memory corruption issue was addressed with improved bounds checking. This issue is fixed in tvOS 18.4.1, visionOS 2.4.1, iOS iOS 18.4.1 and iPadOS 18.4.1, macOS Sequoia 15.4.1. Processing an audio stream in a maliciously crafted media file may result in code execution. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on iOS. **CVE ID: CVE-2025-31200**	https://support.apple.com/en-us/122282, https://support.apple.com/en-us/122400, https://support.apple.com/en-us/122401, https://support.apple.com/en-us/122402	O-APP-TVOS-050525/273
N/A	16-Apr-2025	6.8	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 18.4.1, visionOS 2.4.1, iOS iOS 18.4.1 and iPadOS 18.4.1, macOS Sequoia 15.4.1. An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on iOS. **CVE ID: CVE-2025-31201**	https://support.apple.com/en-us/122282, https://support.apple.com/en-us/122400, https://support.apple.com/en-us/122401, https://support.apple.com/en-us/122402	O-APP-TVOS-050525/274
Product: visionos					
Affected Version(s): * Up to (excluding) 2.3					
NULL	29-Apr-2025	5.7	A null pointer dereference	https://support.	O-APP-VISI-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			was addressed with improved input validation. This issue is fixed in iOS 18.3 and iPadOS 18.3, visionOS 2.3, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, macOS Sequoia 15.3, tvOS 18.3. An attacker on the local network may be able to cause a denial-of-service. **CVE ID: CVE-2025-24179**	apple.com/en-us/122066, https://support.apple.com/en-us/122068, https://support.apple.com/en-us/122072, https://support.apple.com/en-us/122073, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122374	050525/275
Affected Version(s): * Up to (excluding) 2.4					
Use After Free	29-Apr-2025	9.8	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to corrupt process memory. **CVE ID: CVE-2025-24252**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-VISI-050525/276
Incorrect Authorization	29-Apr-2025	7.7	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to bypass authentication policy. **CVE ID: CVE-2025-24206**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375,	O-APP-VISI-050525/277

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/122377	
NULL Pointer Dereference	29-Apr-2025	6.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, watchOS 11.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-24251**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122376	O-APP-VISI-050525/278
Exposure of Sensitive Information to an Unauthorized Actor	29-Apr-2025	5.7	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may be able to leak sensitive user information. **CVE ID: CVE-2025-24270**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-VISI-050525/279
Use After Free	29-Apr-2025	5.7	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination.	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.	O-APP-VISI-050525/280

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-31197	apple.com/en-us/122375, https://support.apple.com/en-us/122377	
Missing Authentication for Critical Function	29-Apr-2025	5.4	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, visionOS 2.4. An unauthenticated user on the same network as a signed-in Mac could send it AirPlay commands without pairing. **CVE ID: CVE-2025-24271**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122377	O-APP-VISI-050525/281
Affected Version(s): * Up to (excluding) 2.4.1					
Out-of-bounds Write	16-Apr-2025	7.5	A memory corruption issue was addressed with improved bounds checking. This issue is fixed in tvOS 18.4.1, visionOS 2.4.1, iOS iOS 18.4.1 and iPadOS 18.4.1, macOS Sequoia 15.4.1. Processing an audio stream in a maliciously crafted media file may result in code execution. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on iOS. **CVE ID: CVE-2025-31200**	https://support.apple.com/en-us/122282, https://support.apple.com/en-us/122400, https://support.apple.com/en-us/122401, https://support.apple.com/en-us/122402	O-APP-VISI-050525/282
N/A	16-Apr-2025	6.8	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 18.4.1, visionOS 2.4.1, iOS iOS 18.4.1 and iPadOS 18.4.1, macOS Sequoia 15.4.1. An attacker with arbitrary read and write	https://support.apple.com/en-us/122282, https://support.apple.com/en-us/122400, https://support.apple.com/en-	O-APP-VISI-050525/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			capability may be able to bypass Pointer Authentication. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on iOS. **CVE ID: CVE-2025-31201**	us/122401, https://support.apple.com/en-us/122402	
Product: watchos					
Affected Version(s): * Up to (excluding) 11.4					
NULL Pointer Dereference	29-Apr-2025	6.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, tvOS 18.4, macOS Ventura 13.7.5, iPadOS 17.7.6, macOS Sonoma 14.7.5, iOS 18.4 and iPadOS 18.4, watchOS 11.4, visionOS 2.4. An attacker on the local network may cause an unexpected app termination. **CVE ID: CVE-2025-24251**	https://support.apple.com/en-us/122371, https://support.apple.com/en-us/122372, https://support.apple.com/en-us/122373, https://support.apple.com/en-us/122374, https://support.apple.com/en-us/122375, https://support.apple.com/en-us/122376	O-APP-WATC-050525/284
Vendor: Broadcom					
Product: fabric_operating_system					
Affected Version(s): From (including) 9.1.0 Up to (excluding) 9.1.1d7					
Improper Control of Generation of Code ('Code Injection')	24-Apr-2025	6.7	Brocade Fabric OS versions starting with 9.1.0 have root access removed, however, a local user with admin privilege can potentially execute arbitrary code with full root privileges on Fabric OS versions 9.1.0 through 9.1.1d6. **CVE ID: CVE-2025-1976**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25602	O-BRO-FABR-050525/285
Vendor: Dlink					
Product: dir-816_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.10_b05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Apr-2025	6.5	D-Link DIR-816 A2V1.1.0B05 was found to contain a command injection in /goform/delRouting. **CVE ID: CVE-2025-29743**	N/A	O-DLI-DIR--050525/286
Product: dir-823x_firmware					
Affected Version(s): 240802					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Apr-2025	9.8	An issue in dlink DIR 823x 240802 allows a remote attacker to execute arbitrary code via the target_addr key value and the function 0x41710c **CVE ID: CVE-2025-29041**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--050525/287
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Apr-2025	9.8	An issue in dlink DIR 832x 240802 allows a remote attacker to execute arbitrary code via the macaddr key value to the function 0x42232c **CVE ID: CVE-2025-29042**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--050525/288
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Apr-2025	9.8	An issue in dlink DIR 832x 240802 allows a remote attacker to execute arbitrary code via the function 0x417234 **CVE ID: CVE-2025-29043**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--050525/289
Improper Neutralization of Special Elements used in an OS Command ('OS Command	17-Apr-2025	9.8	An issue in dlink DIR 823x 240802 allows a remote attacker to execute arbitrary code via the target_addr key value and the function 0x41737c **CVE ID: CVE-2025-29040**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--050525/290

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Injection')					
Improper Control of Generation of Code ('Code Injection')	17-Apr-2025	7.2	An issue in dlink DIR 832x 240802 allows a remote attacker to execute arbitrary code via the function 0x41dda8 **CVE ID: CVE-2025-29039**	N/A	O-DLI-DIR--050525/291
Vendor: infodraw					
Product: pmrs-102_firmware					
Affected Version(s): 7.1.0.0					
Path Traversal: '../filedir'	20-Apr-2025	5.8	In Infodraw Media Relay Service (MRS) 7.1.0.0, the MRS web server (on port 12654) allows reading arbitrary files via ../ directory traversal in the username field. Reading ServerParameters.xml may reveal administrator credentials in cleartext or with MD5 hashing. **CVE ID: CVE-2025-43928**	N/A	O-INF-PMRS-050525/292
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
N/A	25-Apr-2025	8.8	Commvault Web Server has an unspecified vulnerability that can be exploited by a remote, authenticated attacker. According to the Commvault advisory: "Webservers can be compromised through bad actors creating and executing webshells." Fixed in version 11.36.46, 11.32.89, 11.28.141, and 11.20.217 for Windows and Linux platforms. This vulnerability was added to the CISA Known Exploited Vulnerabilities (KEV) Catalog on 2025-04-28. **CVE ID: CVE-2025-3928**	https://documentation.commvault.com/securityadvisories/CV_2025_03_1.html, https://www.commvault.com/blogs/notice-security-advisory-update, https://www.commvault.com/blogs/security-advisory-march-7-2025	O-LIN-LINU-050525/293

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 6.1.134					
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix session use-after-free in multichannel connection There is a race condition between session setup and ksmbd_sessions_deregister. The session can be freed before the connection is added to channel list of session. This patch check reference count of session before freeing it. **CVE ID: CVE-2025-22040**	https://git.kernel.org/stable/c/3980770cb1470054e6400fd9766866597572673 7, https://git.kernel.org/stable/c/596407adb9af1ee75fe7c7529607783d31b66e7f, https://git.kernel.org/stable/c/7dfbd4c43eed91dd2548a95236908025707a8dfd	O-LIN-LINU-050525/294
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in ksmbd_sessions_deregister( ) In multichannel mode, UAF issue can occur in session_deregister when the second channel sets up a session through the connection of the first channel. session that is freed through the global session table can be accessed again through ->sessions of connection. **CVE ID: CVE-2025-22041**	https://git.kernel.org/stable/c/15a9605f8d69dc85005b1a00c31a050b8625e1aa, https://git.kernel.org/stable/c/33cc29e221df7a3085ae413e8c26c4e81a151153, https://git.kernel.org/stable/c/8ed0e9d2f410f63525afb8351181eea36c80bcf1	O-LIN-LINU-050525/295
Out-of-bounds Read	16-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate zero num_subauth before sub_auth is accessed	https://git.kernel.org/stable/c/0e36a3e080d6d8bd7a34e089345d043da4ac8283, https://git.kernel.org/stable/c/	O-LIN-LINU-050525/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Access psid->sub_auth[psid->num_subauth - 1] without checking if num_subauth is non-zero leads to an out-of-bounds read. This patch adds a validation step to ensure num_subauth != 0 before sub_auth is accessed. **CVE ID: CVE-2025-22038**	3ac65de111c686c95316ade660f8ba7aea3cd3cc, https://git.kernel.org/stable/c/56de7778a48560278c334077ace7b9ac4bfb2fd1	
Affected Version(s): * Up to (excluding) 6.1.135					
Use After Free	18-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: HSI: ssi_protocol: Fix use after free vulnerability in ssi_protocol Driver Due to Race Condition In the ssi_protocol_probe() function, &ssi->work is bound with ssip_xmit_work(), In ssip_pn_setup(), the ssip_pn_xmit() function within the ssip_pn_ops structure is capable of starting the work. If we remove the module which will call ssi_protocol_remove() to make a cleanup, it will free ssi through kfree(ssi), while the work mentioned above will be used. The sequence of operations that may lead to a UAF bug is as follows: CPU0 CPU1 | ssip_xmit_work ssi_protocol_remove | kfree(ssi); |	https://git.kernel.org/stable/c/4b4194c9a7a8f92db39e8e86c85f4fb12ebbec4f, https://git.kernel.org/stable/c/58eb29dba712ab0f13af59ca2fe545f5ce360e78, https://git.kernel.org/stable/c/834e602d0cc7c743bfce734fad4a46cefc0f9ab1	O-LIN-LINU-050525/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			| struct hsi_client *cl = ssi->cl; | // use ssi Fix it by ensuring that the work is canceled before proceeding with the cleanup in ssi_protocol_remove(). **CVE ID: CVE-2025-37838**		
Affected Version(s): * Up to (excluding) 6.12.23					
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix null pointer dereference in alloc_preauth_hash() The Client send malformed smb2 negotiate request. ksmbd return error response. Subsequently, the client can send smb2 session setup even thought conn->preauth_info is not allocated. This patch add KSMBD_SESS_NEED_SETUP status of connection to ignore session setup request if smb2 negotiate phase is not complete. **CVE ID: CVE-2025-22037**	https://git.kernel.org/stable/c/8f216b33a5e1b3489c073b1ea1b3d7cb63c8dc4d, https://git.kernel.org/stable/c/b8eb243e670ecf30e91524dd12f7260dac07d335, https://git.kernel.org/stable/c/c8b5b7c5da7d0c31c9b7190b4a7bba5281fc4780	O-LIN-LINU-050525/298
Affected Version(s): 5.10					
NULL Pointer Dereference	17-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_get_echo_skb(): prevent call to kfree_skb() in hard IRQ context If a driver calls can_get_echo_skb() during a hardware IRQ (which is	https://git.kernel.org/stable/c/2283f79b22684d2812e5c76fc2280aae00390365, https://git.kernel.org/stable/c/248b71ce92d4f3a574b2537f9838f48e892618f4,	O-LIN-LINU-050525/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			often, but not always, the case), the 'WARN_ON(in_irq)' in net/core/skbuff.c#skb_release_head_state() might be triggered, under network congestion circumstances, together with the potential risk of a NULL pointer dereference. The root cause of this issue is the call to kfree_skb() instead of dev_kfree_skb_irq() in net/core/dev.c#enqueue_to_backlog(). This patch prevents the skb to be freed within the call to netif_rx() by incrementing its reference count with skb_get(). The skb is finally freed by one of the in-irq-context safe functions: dev_consume_skb_any() or dev_kfree_skb_any(). The "any" version is used because some drivers might call can_get_echo_skb() in a normal context. The reason for this issue to occur is that initially, in the core network stack, loopback skb were not supposed to be received in hardware IRQ context. The CAN stack is an exeption. This bug was previously reported back in 2017 in [1] but the proposed patch never got accepted. While [1] directly modifies net/core/dev.c, we try to propose here a smoother modification local	https://git.kernel.org/stable/c/3a922a85701939624484e7f2fd07d32beed00d25	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to CAN network stack (the assumption behind is that only CAN devices are affected by this issue). [1] http://lore.kernel.org/r/57a3ffb6-3309-3ad5-5a34-e93c3fe3614d@cetitec.com **CVE ID: CVE-2020-36789**		
Affected Version(s): 5.11					
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: peak_usb: fix use after free bugs After calling peak_usb_netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the can_frame cf which aliases skb memory is accessed after the peak_usb_netif_rx_ni(). Reordering the lines solves the issue. **CVE ID: CVE-2021-47670**	https://git.kernel.org/stable/c/50aca891d7a554db0901b245167cd653d73aaa71, https://git.kernel.org/stable/c/5408824636fa0dfedb9ecb0d94abd573131bfbbe, https://git.kernel.org/stable/c/ddd1416f44130377798c1430b76503513b7497c2	O-LIN-LINU-050525/300
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_restart: fix use after free bug After calling netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the can_frame cf which aliases skb memory is accessed after the netif_rx_ni() in: stats->rx_bytes += cf->len; Reordering the lines solves	https://git.kernel.org/stable/c/03f16c5075b22c8902d2af739969e878b0879c94, https://git.kernel.org/stable/c/08ab951787098ae0b6c0364aeea7a8138226f234, https://git.kernel.org/stable/c/260925a0b7d2da5449f8ecfd02c1405e0c8a45b8	O-LIN-LINU-050525/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the issue. **CVE ID: CVE-2021-47668**		
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: vxcan: vxcan_xmit: fix use after free bug After calling netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the canfd_frame cfd which aliases skb memory is accessed after the netif_rx_ni(). **CVE ID: CVE-2021-47669**	https://git.kernel.org/stable/c/6d6dcf2399cdd26f7f5426ca8dd8366b7f2ca105, https://git.kernel.org/stable/c/75854cad5d80976f6ea0f0431f8cedd3bcc475cb, https://git.kernel.org/stable/c/9b820875a32a3443d67bfd368e93038354e98052	O-LIN-LINU-050525/302
Affected Version(s): From (including) 2.6.19 Up to (excluding) 5.10.236					
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: ext4: fix OOB read when checking dotdot dir Mounting a corrupted filesystem with directory which contains '.' dir entry with rec_len == block size results in out-of-bounds read (later on, when the corrupted directory is removed). ext4_empty_dir() assumes every ext4 directory contains at least '.' and '..' as directory entries in the first data block. It first loads the '.' dir entry, performs sanity checks by calling ext4_check_dir_entry() and then uses its rec_len member to compute the location of '..' dir entry (in ext4_next_entry). It assumes the '..' dir entry fits into the	https://git.kernel.org/stable/c/52a5509ab19a5d3afe301165d9b5787bba34d842, https://git.kernel.org/stable/c/53bc45da8d8da92ec07877f5922b130562eb4b00, https://git.kernel.org/stable/c/89503e5eae64637d0fa2218912b54660effe7d93	O-LIN-LINU-050525/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			same data block. If the rec_len of '.' is precisely one block (4KB), it slips through the sanity checks (it is considered the last directory entry in the data block) and leaves "struct ext4_dir_entry_2 *de" point exactly past the memory slot allocated to the data block. The following call to ext4_check_dir_entry() on new value of de then dereferences this pointer which results in out-of-bounds mem access. Fix this by extending __ext4_check_dir_entry() to check for '.' dir entries that reach the end of data block. Make sure to ignore the phony dir entries for checksum (by checking name_len for non-zero). Note: This is reported by KASAN as use-after-free in case another structure was recently freed from the slot past the bound, but it is really an OOB read. This issue was found by syzkaller tool. Call Trace: [38.594108] BUG: KASAN: slab-use-after-free in __ext4_check_dir_entry+0x67e/0x710 [38.594649] Read of size 2 at addr ffff88802b41a004 by task syz-executor/5375 [38.595158] [38.595288] CPU: 0 UID: 0 PID: 5375 Comm: syz-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executor Not tainted 6.14.0-rc7 #1 [38.595298] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [38.595304] Call Trace: [38.595308] <TASK> [38.595311] dump_stack_lvl+0xa7/0xd0 [38.595325] print_address_description.constprop.0+0x2c/0x3f0 [38.595339] ? __ext4_check_dir_entry+0x67e/0x710 [38.595349] print_report+0xaa/0x250 [38.595359] ? __ext4_check_dir_entry+0x67e/0x710 [38.595368] ? kasan_addr_to_slab+0x9/0x90 [38.595378] kasan_report+0xab/0xe0 [38.595389] ? __ext4_check_dir_entry+0x67e/0x710 [38.595400] __ext4_check_dir_entry+0x67e/0x710 [38.595410] ext4_empty_dir+0x465/0x990 [38.595421] ? __pfx_ext4_empty_dir+0x10/0x10 [38.595432] ext4_rmdir.part.0+0x29a/0xd10 [38.595441] ? __dquot_initialize+0x2a7/0xbf0 [38.595455] ? __pfx_ext4_rmdir.part.0+0x10/0x10 [38.595464] ? __pfx___dquot_initialize+0x1		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0/0x10 [38.595478] ? down_write+0xdb/0x140 [38.595487] ? __pfx_down_write+0x10/0x10 [38.595497] ext4_rmdir+0xee/0x140 [38.595506] vfs_rmdir+0x209/0x670 [38.595517] ? lookup_one_qstr_excl+0x3b/0x190 [38.595529] do_rmdir+0x363/0x3c0 [38.595537] ? __pfx_do_rmdir+0x10/0x10 [38.595544] ? strncpy_from_user+0x1ff/0x2e0 [38.595561] __x64_sys_unlinkat+0xf0/0x130 [38.595570] do_syscall_64+0x5b/0x180 [38.595583] entry_SYSCALL_64_after_hwframe+0x76/0x7e **CVE ID: CVE-2025-37785**		
Affected Version(s): From (including) 2.6.31 Up to (excluding) 4.4.244					
NULL Pointer Dereference	17-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_get_echo_skb(): prevent call to kfree_skb() in hard IRQ context If a driver calls can_get_echo_skb() during a hardware IRQ (which is often, but not always, the case), the 'WARN_ON(in_irq)' in net/core/skbuff.c#skb_release_head_state() might be triggered, under network congestion circumstances, together with the potential	https://git.kernel.org/stable/c/2283f79b22684d2812e5c76fc2280aae00390365, https://git.kernel.org/stable/c/248b71ce92d4f3a574b2537f9838f48e892618f4, https://git.kernel.org/stable/c/3a922a85701939624484e7f2fd07d32beed00d25	O-LIN-LINU-050525/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			risk of a NULL pointer dereference. The root cause of this issue is the call to kfree_skb() instead of dev_kfree_skb_irq() in net/core/dev.c#enqueue_to_backlog(). This patch prevents the skb to be freed within the call to netif_rx() by incrementing its reference count with skb_get(). The skb is finally freed by one of the in-irq-context safe functions: dev_consume_skb_any() or dev_kfree_skb_any(). The "any" version is used because some drivers might call can_get_echo_skb() in a normal context. The reason for this issue to occur is that initially, in the core network stack, loopback skb were not supposed to be received in hardware IRQ context. The CAN stack is an exeption. This bug was previously reported back in 2017 in [1] but the proposed patch never got accepted. While [1] directly modifies net/core/dev.c, we try to propose here a smoother modification local to CAN network stack (the assumption behind is that only CAN devices are affected by this issue). [1] http://lore.kernel.org/r/57		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a3ffb6-3309-3ad5-5a34-e93c3fe3614d@cetitec.com **CVE ID: CVE-2020-36789**		
Affected Version(s): From (including) 2.6.31 Up to (excluding) 4.4.254					
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_restart: fix use after free bug After calling netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the can_frame cf which aliases skb memory is accessed after the netif_rx_ni() in: stats->rx_bytes += cf->len; Reordering the lines solves the issue. **CVE ID: CVE-2021-47668**	https://git.kernel.org/stable/c/03f16c5075b22c8902d2af739969e878b0879c94, https://git.kernel.org/stable/c/08ab951787098ae0b6c0364aeea7a8138226f234, https://git.kernel.org/stable/c/260925a0b7d2da5449f8ecfd02c1405e0c8a45b8	O-LIN-LINU-050525/305
Affected Version(s): From (including) 3.1 Up to (excluding) 6.14.2					
N/A	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: jfs: reject on-disk inodes of an unsupported type Syzbot has reported the following BUG: kernel BUG at fs/inode.c:668! Oops: invalid opcode: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 3 UID: 0 PID: 139 Comm: jfsCommit Not tainted 6.12.0-rc4-syzkaller-00085-g4e46774408d9 #0 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-3.fc41	https://git.kernel.org/stable/c/8987891c4653874d5e3f5d11f063912f4e0b58eb, https://git.kernel.org/stable/c/8c3f9a70d2d4dd6c640afe294b05c6a0a45434d9	O-LIN-LINU-050525/306

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			04/01/2014 RIP: 0010:clear_inode+0x168/0x190 Code: 4c 89 f7 e8 ba fe e5 ff e9 61 ff ff ff 44 89 f1 80 e1 07 80 c1 03 38 c1 7c c1 4c 89 f7 e8 90 ff e5 ff eb b7 0b e8 01 5d 7f ff 90 0f 0b e8 f9 5c 7f ff 90 0f 0b e8 f1 5c 7f RSP: 0018:ffffc900027dfae8 EFLAGS: 00010093 RAX: ffffffff82157a87 RBX: 0000000000000001 RCX: ffff888104d4b980 RDX: 0000000000000000 RSI: 0000000000000001 RDI: 0000000000000000 RBP: ffffc900027dfc90 R08: ffffffff82157977 R09: fffff520004fbf38 R10: dffffc0000000000 R11: fffff520004fbf38 R12: dffffc0000000000 R13: ffff88811315bc00 R14: ffff88811315bda8 R15: ffff88811315bb80 FS: 0000000000000000(0000) GS:ffff888135f00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00005565222e0578 CR3: 0000000026ef0000 CR4: 00000000000006f0 Call Trace: <TASK> ? __die_body+0x5f/0xb0 ? die+0x9e/0xc0 ? do_trap+0x15a/0x3a0 ? clear_inode+0x168/0x190 ? do_error_trap+0x1dc/0x2c0 ? clear_inode+0x168/0x190 ? __pfx_do_error_trap+0x10/0x10 ? report_bug+0x3cd/0x500		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? handle_invalid_op+0x34/0x40 ? clear_inode+0x168/0x190 ? exc_invalid_op+0x38/0x50 ? asm_exc_invalid_op+0x1a/0x20 ? clear_inode+0x57/0x190 ? clear_inode+0x167/0x190 ? clear_inode+0x168/0x190 ? clear_inode+0x167/0x190 jfs_evict_inode+0xb5/0x440 ? __pfx_jfs_evict_inode+0x10/0x10 evict+0x4ea/0x9b0 ? __pfx_evict+0x10/0x10 ? iput+0x713/0xa50 txUpdateMap+0x931/0xb10 ? __pfx_txUpdateMap+0x10/0x10 jfs_lazycommit+0x49a/0xb80 ? _raw_spin_unlock_irqrestore+0x8f/0x140 ? lockdep_hardirqs_on+0x99/0x150 ? __pfx_jfs_lazycommit+0x10/0x10 ? __pfx_default_wake_function+0x10/0x10 ? __kthread_parkme+0x169/0x1d0 ? __pfx_jfs_lazycommit+0x10/0x10		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kthread+0x2f2/0x390 ? __pfx_jfs_lazycommit+0x10/ 0x10 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x4d/0x80 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0 x30 </TASK> This happens when 'clear_inode()' makes an attempt to finalize an underlying JFS inode of unknown type. According to JFS layout description from https://jfs.sourceforge.net/project/pub/jfslayout.pdf, inode types from 5 to 15 are reserved for future extensions and should not be encountered on a valid filesystem. So add an extra check for valid inode type in 'copy_from_dinode()'. **CVE ID: CVE-2025-37925**		
Affected Version(s): From (including) 3.18 Up to (excluding) 5.4.292					
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: thermal: int340x: Add NULL check for adev Not all devices have an ACPI companion fwnode, so adev might be NULL. This is similar to the commit cd2fd6eab480 ("platform/x86: int3472: Check for adev == NULL"). Add a check for adev not being set and return -ENODEV in that case to avoid a possible NULL pointer deref in	https://git.kernel.org/stable/c/0c49f12c77b77a706fd41370c11910635e491845, https://git.kernel.org/stable/c/2542a3f70e563a9e70e7ded314286535a3321bdb, https://git.kernel.org/stable/c/3155d5261b518776d1b807d9d922669991bbee56	O-LIN-LINU-050525/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			int3402_thermal_probe(). Note, under the same directory, int3400_thermal_probe() has such a check. [rjw: Subject edit, added Fixes:] **CVE ID: CVE-2025-23136**		
Affected Version(s): From (including) 4.0 Up to (excluding) 4.19.171					
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: peak_usb: fix use after free bugs After calling peak_usb_netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the can_frame cf which aliases skb memory is accessed after the peak_usb_netif_rx_ni(). Reordering the lines solves the issue. **CVE ID: CVE-2021-47670**	https://git.kernel.org/stable/c/50aca891d7a554db0901b245167cd653d73aaa71, https://git.kernel.org/stable/c/5408824636fa0dfedb9ecb0d94abd573131bfbbe, https://git.kernel.org/stable/c/ddd1416f44130377798c1430b76503513b7497c2	O-LIN-LINU-050525/308
Affected Version(s): From (including) 4.10 Up to (excluding) 4.14.207					
NULL Pointer Dereference	17-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_get_echo_skb(): prevent call to kfree_skb() in hard IRQ context If a driver calls can_get_echo_skb() during a hardware IRQ (which is often, but not always, the case), the 'WARN_ON(in_irq)' in net/core/skbuff.c#skb_rele	https://git.kernel.org/stable/c/2283f79b22684d2812e5c76fc2280aae00390365, https://git.kernel.org/stable/c/248b71ce92d4f3a574b2537f9838f48e892618f4, https://git.kernel.org/stable/c/3a922a85701939624484e7f2fd0	O-LIN-LINU-050525/309

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ase_head_state() might be triggered, under network congestion circumstances, together with the potential risk of a NULL pointer dereference. The root cause of this issue is the call to kfree_skb() instead of dev_kfree_skb_irq() in net/core/dev.c#enqueue_to_backlog(). This patch prevents the skb to be freed within the call to netif_rx() by incrementing its reference count with skb_get(). The skb is finally freed by one of the in-irq-context safe functions: dev_consume_skb_any() or dev_kfree_skb_any(). The "any" version is used because some drivers might call can_get_echo_skb() in a normal context. The reason for this issue to occur is that initially, in the core network stack, loopback skb were not supposed to be received in hardware IRQ context. The CAN stack is an exeption. This bug was previously reported back in 2017 in [1] but the proposed patch never got accepted. While [1] directly modifies net/core/dev.c, we try to propose here a smoother modification local to CAN network stack (the assumption behind is that only CAN devices are affected by this	7d32beed00d25	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue). [1] http://lore.kernel.org/r/57a3ffb6-3309-3ad5-5a34-e93c3fe3614d@cetitec.com **CVE ID: CVE-2020-36789**		
Affected Version(s): From (including) 4.10 Up to (excluding) 4.14.218					
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_restart: fix use after free bug After calling netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the can_frame cf which aliases skb memory is accessed after the netif_rx_ni() in: stats->rx_bytes += cf->len; Reordering the lines solves the issue. **CVE ID: CVE-2021-47668**	https://git.kernel.org/stable/c/03f16c5075b22c8902d2af739969e878b0879c94, https://git.kernel.org/stable/c/08ab951787098ae0b6c0364aeea7a8138226f234, https://git.kernel.org/stable/c/260925a0b7d2da5449f8ecfd02c1405e0c8a45b8	O-LIN-LINU-050525/310
Affected Version(s): From (including) 4.12 Up to (excluding) 4.14.218					
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: vxcan: vxcan_xmit: fix use after free bug After calling netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the canfd_frame cfd which aliases skb memory is accessed after the netif_rx_ni(). **CVE ID: CVE-2021-47669**	https://git.kernel.org/stable/c/6d6dcf2399cdd26f7f5426ca8dd8366b7f2ca105, https://git.kernel.org/stable/c/75854cad5d80976f6ea0f0431f8cedd3bcc475cb, https://git.kernel.org/stable/c/9b820875a32a3443d67bfd368e930383549805 2	O-LIN-LINU-050525/311
Affected Version(s): From (including) 4.14.324 Up to (excluding) 4.15					
Use After	16-Apr-2025	7.8	In the Linux kernel, the	https://git.kern	O-LIN-LINU-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

Free			following vulnerability has been resolved:
			
			tracing: Fix use-after-free in print_graph_function_flags during tracer switching
			
			Kairui reported a UAF issue in print_graph_function_flags() during ftrace stress testing [1]. This issue can be reproduced if puting a 'mdelay(10)' after 'mutex_unlock(&trace_types_lock)' in s_start(), and executing the following script:
			
			$ echo function_graph > current_tracer
			$ cat trace > /dev/null &
			$ sleep 5 # Ensure the 'cat' reaches the 'mdelay(10)' point
			$ echo timerlat > current_tracer
			
			The root cause lies in the two calls to print_graph_function_flags within print_trace_line during each s_show():
			
			* One through 'iter->trace->print_line()';
			* Another through 'event->funcs->trace()', which is hidden in print_trace_fmt() before print_trace_line returns.
			
			Tracer switching only updates the former, while the latter continues to use the print_line function of the old tracer, which in the script above is print_graph_function_flags.
				el.org/stable/c/099ef3385800828b74933a96c117574637c3fb3a, https://git.kernel.org/stable/c/42561fe62c3628ea3bc9623f64f047605e98857f, https://git.kernel.org/stable/c/70be951bc01e4a0e10d443f3510bb17426f257fb	050525/312

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Moreover, when switching from the 'function_graph' tracer to the 'timerlat' tracer, s_start only calls graph_trace_close of the 'function_graph' tracer to free 'iter->private', but does not set it to NULL. This provides an opportunity for 'event->funcs->trace()' to use an invalid 'iter->private'. To fix this issue, set 'iter->private' to NULL immediately after freeing it in graph_trace_close(), ensuring that an invalid pointer is not passed to other tracers. Additionally, clean up the unnecessary 'iter->private = NULL' during each 'cat trace' when using wakeup and irqsoff tracers. [1] https://lore.kernel.org/all/20231112150030.84609-1-ryncsn@gmail.com/ **CVE ID: CVE-2025-22035**		
Affected Version(s): From (including) 4.15 Up to (excluding) 4.19.158					
NULL Pointer Dereference	17-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_get_echo_skb(): prevent call to kfree_skb() in hard IRQ context If a driver calls can_get_echo_skb() during a hardware IRQ (which is often, but not always, the case), the	https://git.kernel.org/stable/c/2283f79b22684d2812e5c76fc2280aae00390365, https://git.kernel.org/stable/c/248b71ce92d4f3a574b2537f9838f48e892618f4, https://git.kernel.org/stable/c/	O-LIN-LINU-050525/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'WARN_ON(in_irq)' in net/core/skbuff.c#skb_release_head_state() might be triggered, under network congestion circumstances, together with the potential risk of a NULL pointer dereference. The root cause of this issue is the call to kfree_skb() instead of dev_kfree_skb_irq() in net/core/dev.c#enqueue_to_backlog(). This patch prevents the skb to be freed within the call to netif_rx() by incrementing its reference count with skb_get(). The skb is finally freed by one of the in-irq-context safe functions: dev_consume_skb_any() or dev_kfree_skb_any(). The "any" version is used because some drivers might call can_get_echo_skb() in a normal context. The reason for this issue to occur is that initially, in the core network stack, loopback skb were not supposed to be received in hardware IRQ context. The CAN stack is an exeption. This bug was previously reported back in 2017 in [1] but the proposed patch never got accepted. While [1] directly modifies net/core/dev.c, we try to propose here a smoother modification local to CAN network stack (the assumption	3a922a85701939624484e7f2fd07d32beed00d25	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behind is that only CAN devices are affected by this issue). [1] http://lore.kernel.org/r/57a3ffb6-3309-3ad5-5a34-e93c3fe3614d@cetitec.com **CVE ID: CVE-2020-36789**		
Affected Version(s): From (including) 4.15 Up to (excluding) 4.19.171					
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_restart: fix use after free bug After calling netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the can_frame cf which aliases skb memory is accessed after the netif_rx_ni() in: stats->rx_bytes += cf->len; Reordering the lines solves the issue. **CVE ID: CVE-2021-47668**	https://git.kernel.org/stable/c/03f16c5075b22c8902d2af739969e878b0879c94, https://git.kernel.org/stable/c/08ab951787098ae0b6c0364aeea7a8138226f234, https://git.kernel.org/stable/c/260925a0b7d2da5449f8ecfd02c1405e0c8a45b8	O-LIN-LINU-050525/314
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: vxcan: vxcan_xmit: fix use after free bug After calling netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the canfd_frame cfd which aliases skb memory is accessed after the netif_rx_ni(). **CVE ID: CVE-2021-47669**	https://git.kernel.org/stable/c/6d6dcf2399cdd26f7f5426ca8dd8366b7f2ca105, https://git.kernel.org/stable/c/75854cad5d80976f6ea0f0431f8cedd3bcc475cb, https://git.kernel.org/stable/c/9b820875a32a3443d67bfd368e930383 54e98052	O-LIN-LINU-050525/315
Affected Version(s): From (including) 4.19.293 Up to (excluding) 4.20					
Use After	16-Apr-2025	7.8	In the Linux kernel, the	https://git.kern	O-LIN-LINU-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

Free			following vulnerability has been resolved:
			
			tracing: Fix use-after-free in print_graph_function_flags during tracer switching
			
			Kairui reported a UAF issue in print_graph_function_flags() during ftrace stress testing [1]. This issue can be reproduced if puting a 'mdelay(10)' after 'mutex_unlock(&trace_types_lock)' in s_start(), and executing the following script:
			
			$ echo function_graph > current_tracer
			$ cat trace > /dev/null &
			$ sleep 5 # Ensure the 'cat' reaches the 'mdelay(10)' point
			$ echo timerlat > current_tracer
			
			The root cause lies in the two calls to print_graph_function_flags within print_trace_line during each s_show():
			
			* One through 'iter->trace->print_line()';
			* Another through 'event->funcs->trace()', which is hidden in print_trace_fmt() before print_trace_line returns.
			
			Tracer switching only updates the former, while the latter continues to use the print_line function of the old tracer, which in the script above is print_graph_function_flags.
				el.org/stable/c/099ef3385800828b74933a96c117574637c3fb3a, https://git.kernel.org/stable/c/42561fe62c3628ea3bc9623f64f047605e98857f, https://git.kernel.org/stable/c/70be951bc01e4a0e10d443f3510bb17426f257fb	050525/316

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Moreover, when switching from the 'function_graph' tracer to the 'timerlat' tracer, s_start only calls graph_trace_close of the 'function_graph' tracer to free 'iter->private', but does not set it to NULL. This provides an opportunity for 'event->funcs->trace()' to use an invalid 'iter->private'. To fix this issue, set 'iter->private' to NULL immediately after freeing it in graph_trace_close(), ensuring that an invalid pointer is not passed to other tracers. Additionally, clean up the unnecessary 'iter->private = NULL' during each 'cat trace' when using wakeup and irqsoff tracers. [1] https://lore.kernel.org/all/20231112150030.84609-1-ryncsn@gmail.com/ **CVE ID: CVE-2025-22035**		
Affected Version(s): From (including) 4.19.302 Up to (excluding) 4.20					
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: arcnet: Add NULL check in com20020pci_probe() devm_kasprintf() returns NULL when memory allocation fails. Currently, com20020pci_probe() does not check for this case, which results in a NULL pointer dereference.	https://git.kernel.org/stable/c/661cf5d102949898c931e81fd4e1c773afcdeafa, https://git.kernel.org/stable/c/887226163504494ea7e58033a97c2d2ab12e05d4, https://git.kernel.org/stable/c/905a34dc1ad9a	O-LIN-LINU-050525/317

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Add NULL check after devm_kasprintf() to prevent this issue and ensure no resources are left allocated. **CVE ID: CVE-2025-22054**	53a8aaaf8a759ea5dbaaa30418d	
Affected Version(s): From (including) 4.19.325 Up to (excluding) 4.20					
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: jfs: fix slab-out-of-bounds read in ea_get() During the "size_check" label in ea_get(), the code checks if the extended attribute list (xattr) size matches ea_size. If not, it logs "ea_get: invalid extended attribute" and calls print_hex_dump(). Here, EALIST_SIZE(ea_buf->xattr) returns 4110417968, which exceeds INT_MAX (2,147,483,647). Then ea_size is clamped: int size = clamp_t(int, ea_size, 0, EALIST_SIZE(ea_buf->xattr)); Although clamp_t aims to bound ea_size between 0 and 4110417968, the upper limit is treated as an int, causing an overflow above 2^31 - 1. This leads "size" to wrap around and become negative (-184549328). The "size" is then passed to print_hex_dump() (called "len" in	https://git.kernel.org/stable/c/0beddc2a3f9b9cf7d8887973041e36c2d0fa3652, https://git.kernel.org/stable/c/16d3d36436492aa248b2d8045e75585ebcc2f34d, https://git.kernel.org/stable/c/3d6fd5b9c6acbc005e53d0211c7381f566babec1	O-LIN-LINU-050525/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			print_hex_dump()), it is passed as type size_t (an unsigned type), this is then stored inside a variable called "int remaining", which is then assigned to "int linelen" which is then passed to hex_dump_to_buffer(). In print_hex_dump() the for loop, iterates through 0 to len-1, where len is 18446744073525002176, calling hex_dump_to_buffer() on each iteration:
			
			for (i = 0; i < len; i += rowsize) {
			linelen = min(remaining, rowsize);
			remaining -= rowsize;
			
			hex_dump_to_buffer (ptr + i, linelen, rowsize, groupsize,
			
			linebuf, sizeof(linebuf), ascii);
			
			...
			}
			
			The expected stopping condition (i < len) is effectively broken since len is corrupted and very large. This eventually leads to the "ptr+i" being passed to hex_dump_to_buffer() to get closer to the end of the actual bounds of "ptr", eventually an out of bounds access is done in hex_dump_to_buffer() in the following		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			for loop:
			
			for (j = 0; j < len; j++) {
			if (linebuflen < lx + 2)
			
			goto overflow2;
			ch = ptr[j];
			...
			}
			
			To fix this we should validate "EALIST_SIZE(ea_buf->xattr)" before it is utilised.
			
			CVE ID: CVE-2025-39735		

Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.78					
NULL Pointer Dereference	17-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_get_echo_skb(): prevent call to kfree_skb() in hard IRQ context If a driver calls can_get_echo_skb() during a hardware IRQ (which is often, but not always, the case), the 'WARN_ON(in_irq)' in net/core/skbuff.c#skb_release_head_state() might be triggered, under network congestion circumstances, together with the potential risk of a NULL pointer dereference. The root cause of this issue is the call to kfree_skb() instead of dev_kfree_skb_irq() in net/core/dev.c#enqueue_to_backlog().	https://git.kernel.org/stable/c/2283f79b22684d2812e5c76fc2280aae00390365, https://git.kernel.org/stable/c/248b71ce92d4f3a574b2537f9838f48e892618f4, https://git.kernel.org/stable/c/3a922a85701939624484e7f2fd07d32beed00d25	O-LIN-LINU-050525/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This patch prevents the skb to be freed within the call to netif_rx() by incrementing its reference count with skb_get(). The skb is finally freed by one of the in-irq-context safe functions: dev_consume_skb_any() or dev_kfree_skb_any(). The "any" version is used because some drivers might call can_get_echo_skb() in a normal context. The reason for this issue to occur is that initially, in the core network stack, loopback skb were not supposed to be received in hardware IRQ context. The CAN stack is an exeption. This bug was previously reported back in 2017 in [1] but the proposed patch never got accepted. While [1] directly modifies net/core/dev.c, we try to propose here a smoother modification local to CAN network stack (the assumption behind is that only CAN devices are affected by this issue). [1] http://lore.kernel.org/r/57a3ffb6-3309-3ad5-5a34-e93c3fe3614d@cetitec.com **CVE ID: CVE-2020-36789**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.93					
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/50aca891d7a554db0901b24516	O-LIN-LINU-050525/320

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can: peak_usb: fix use after free bugs After calling peak_usb_netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the can_frame cf which aliases skb memory is accessed after the peak_usb_netif_rx_ni(). Reordering the lines solves the issue. **CVE ID: CVE-2021-47670**	7cd653d73aaa71, https://git.kernel.org/stable/c/5408824636fa0dfedb9ecb0d94abd573131bfbbe, https://git.kernel.org/stable/c/ddd1416f44130377798c1430b76503513b7497c2	
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_restart: fix use after free bug After calling netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the can_frame cf which aliases skb memory is accessed after the netif_rx_ni() in: stats->rx_bytes += cf->len; Reordering the lines solves the issue. **CVE ID: CVE-2021-47668**	https://git.kernel.org/stable/c/03f16c5075b22c8902d2af739969e878b0879c94, https://git.kernel.org/stable/c/08ab951787098ae0b6c0364aeea7a8138226f234, https://git.kernel.org/stable/c/260925a0b7d2da5449f8ecfd02c1405e0c8a45b8	O-LIN-LINU-050525/321
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: vxcan: vxcan_xmit: fix use after free bug After calling netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the canfd_frame cfd which aliases skb memory is accessed after the netif_rx_ni().	https://git.kernel.org/stable/c/6d6dcf2399cdd26f7f5426ca8dd8366b7f2ca105, https://git.kernel.org/stable/c/75854cad5d80976f6ea0f0431f8cedd3bcc475cb, https://git.kernel.org/stable/c/9b820875a32a3443d67bfd368e	O-LIN-LINU-050525/322

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2021-47669	93038354e98052	
Affected Version(s): From (including) 4.5 Up to (excluding) 4.9.244					
NULL Pointer Dereference	17-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_get_echo_skb(): prevent call to kfree_skb() in hard IRQ context If a driver calls can_get_echo_skb() during a hardware IRQ (which is often, but not always, the case), the 'WARN_ON(in_irq)' in net/core/skbuff.c#skb_release_head_state() might be triggered, under network congestion circumstances, together with the potential risk of a NULL pointer dereference. The root cause of this issue is the call to kfree_skb() instead of dev_kfree_skb_irq() in net/core/dev.c#enqueue_to_backlog(). This patch prevents the skb to be freed within the call to netif_rx() by incrementing its reference count with skb_get(). The skb is finally freed by one of the in-irq-context safe functions: dev_consume_skb_any() or dev_kfree_skb_any(). The "any" version is used because some drivers might call can_get_echo_skb() in a normal context. The reason for this issue to occur is that initially, in the	https://git.kernel.org/stable/c/2283f79b22684d2812e5c76fc2280aae00390365, https://git.kernel.org/stable/c/248b71ce92d4f3a574b2537f9838f48e892618f4, https://git.kernel.org/stable/c/3a922a85701939624484e7f2fd07d32beed00d25	O-LIN-LINU-050525/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			core network stack, loopback skb were not supposed to be received in hardware IRQ context. The CAN stack is an exeption. This bug was previously reported back in 2017 in [1] but the proposed patch never got accepted. While [1] directly modifies net/core/dev.c, we try to propose here a smoother modification local to CAN network stack (the assumption behind is that only CAN devices are affected by this issue). [1] http://lore.kernel.org/r/57a3ffb6-3309-3ad5-5a34-e93c3fe3614d@cetitec.com **CVE ID: CVE-2020-36789**		
Affected Version(s): From (including) 4.5 Up to (excluding) 4.9.254					
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_restart: fix use after free bug After calling netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the can_frame cf which aliases skb memory is accessed after the netif_rx_ni() in: stats->rx_bytes += cf->len; Reordering the lines solves the issue. **CVE ID: CVE-2021-47668**	https://git.kernel.org/stable/c/03f16c5075b22c8902d2af739969e878b0879c94, https://git.kernel.org/stable/c/08ab951787098ae0b6c0364aeea7a8138226f234, https://git.kernel.org/stable/c/260925a0b7d2da5449f8ecfd02c1405e0c8a45b8	O-LIN-LINU-050525/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.8 Up to (excluding) 5.4.292					
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netlabel: Fix NULL pointer exception caused by CALIPSO on IPv4 sockets When calling netlbl_conn_setattr(), addr->sa_family is used to determine the function behavior. If sk is an IPv4 socket, but the connect function is called with an IPv6 address, the function calipso_sock_setattr() is triggered. Inside this function, the following code is executed: sk_fullsock(__sk) ? inet_sk(__sk)->pinet6 : NULL; Since sk is an IPv4 socket, pinet6 is NULL, leading to a null pointer dereference. This patch fixes the issue by checking if inet6_sk(sk) returns a NULL pointer before accessing pinet6. **CVE ID: CVE-2025-22063**	https://git.kernel.org/stable/c/078aabd567de3d63d37d7673f714e309d369e6e2, https://git.kernel.org/stable/c/172a8a996a337206970467e871dd995ac07640b1, https://git.kernel.org/stable/c/1927d0bcd5b81e80971bf6b8eba267508bd1c78b	O-LIN-LINU-050525/325
Affected Version(s): From (including) 5.10.193 Up to (excluding) 5.10.236					
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix use-after-free in print_graph_function_flags during tracer switching Kairui reported a UAF issue in print_graph_function_flags() during	https://git.kernel.org/stable/c/099ef3385800828b74933a96c117574637c3fb3a, https://git.kernel.org/stable/c/42561fe62c3628ea3bc9623f64f047605e98857f, https://git.kern	O-LIN-LINU-050525/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			ftrace stress testing [1]. This issue can be reproduced if puting a 'mdelay(10)' after 'mutex_unlock(&trace_types_lock)' in s_start(), and executing the following script:
			
			$ echo function_graph > current_tracer
			$ cat trace > /dev/null &
			$ sleep 5 # Ensure the 'cat' reaches the 'mdelay(10)' point
			$ echo timerlat > current_tracer
			
			The root cause lies in the two calls to print_graph_function_flags within print_trace_line during each s_show():
			
			* One through 'iter->trace->print_line()';
			* Another through 'event->funcs->trace()', which is hidden in print_trace_fmt() before print_trace_line returns.
			
			Tracer switching only updates the former, while the latter continues to use the print_line function of the old tracer, which in the script above is print_graph_function_flags.
			
			Moreover, when switching from the 'function_graph' tracer to the 'timerlat' tracer, s_start only calls graph_trace_close of the 'function_graph' tracer to free 'iter->private', but does not set it to NULL. This provides an opportunity for 'event-
				el.org/stable/c/70be951bc01e4a0e10d443f3510bb17426f257fb	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>funcs->trace()' to use an invalid 'iter->private'. To fix this issue, set 'iter->private' to NULL immediately after freeing it in graph_trace_close(), ensuring that an invalid pointer is not passed to other tracers. Additionally, clean up the unnecessary 'iter->private = NULL' during each 'cat trace' when using wakeup and irqsoff tracers. [1] https://lore.kernel.org/all/20231112150030.84609-1-ryncsn@gmail.com/ **CVE ID: CVE-2025-22035**		
Affected Version(s): From (including) 5.10.204 Up to (excluding) 5.10.236					
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: arcnet: Add NULL check in com20020pci_probe() devm_kasprintf() returns NULL when memory allocation fails. Currently, com20020pci_probe() does not check for this case, which results in a NULL pointer dereference. Add NULL check after devm_kasprintf() to prevent this issue and ensure no resources are left allocated. **CVE ID: CVE-2025-22054**	https://git.kernel.org/stable/c/661cf5d102949898c931e81fd4e1c773afcdeafa, https://git.kernel.org/stable/c/887226163504494ea7e58033a97c2d2ab12e05d4, https://git.kernel.org/stable/c/905a34dc1ad9a53a8aaaf8a759ea5dbaaa30418d	O-LIN-LINU-050525/327
Affected Version(s): From (including) 5.10.231 Up to (excluding) 5.10.236					
Out-of-	18-Apr-2025	7.1	In the Linux kernel, the	https://git.kern	O-LIN-LINU-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
bounds Read			following vulnerability has been resolved: jfs: fix slab-out-of-bounds read in ea_get() During the "size_check" label in ea_get(), the code checks if the extended attribute list (xattr) size matches ea_size. If not, it logs "ea_get: invalid extended attribute" and calls print_hex_dump(). Here, EALIST_SIZE(ea_buf->xattr) returns 4110417968, which exceeds INT_MAX (2,147,483,647). Then ea_size is clamped: int size = clamp_t(int, ea_size, 0, EALIST_SIZE(ea_buf->xattr)); Although clamp_t aims to bound ea_size between 0 and 4110417968, the upper limit is treated as an int, causing an overflow above 2^31 - 1. This leads "size" to wrap around and become negative (-184549328). The "size" is then passed to print_hex_dump() (called "len" in print_hex_dump()), it is passed as type size_t (an unsigned type), this is then stored inside a variable called "int remaining", which is then assigned to "int linelen" which is then passed to hex_dump_to_buffer(). In print_hex_dump()	el.org/stable/c/0beddc2a3f9b9cf7d8887973041e36c2d0fa3652, https://git.kernel.org/stable/c/16d3d36436492aa248b2d8045e75585ebcc2f34d, https://git.kernel.org/stable/c/3d6fd5b9c6acbc005e53d0211c7381f566babec1	050525/328

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			the for loop, iterates through 0 to len-1, where len is 18446744073525002176, calling hex_dump_to_buffer() on each iteration:
			
			for (i = 0; i < len; i += rowsize) {
			linelen = min(remaining, rowsize);
			remaining -= rowsize;
			
			hex_dump_to_buffer (ptr + i, linelen, rowsize, groupsize,
			
			linebuf, sizeof(linebuf), ascii);
			
			...
			}
			
			The expected stopping condition (i < len) is effectively broken since len is corrupted and very large. This eventually leads to the "ptr+i" being passed to hex_dump_to_buffer() to get closer to the end of the actual bounds of "ptr", eventually an out of bounds access is done in hex_dump_to_buffer() in the following for loop:
			
			for (j = 0; j < len; j++) {
			if (linebuflen < lx + 2)
			
			goto overflow2;
			ch = ptr[j];
			...		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			} To fix this we should validate "EALIST_SIZE(ea_buf->xattr)" before it is utilised. **CVE ID: CVE-2025-39735**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.180					
Out-of-bounds Write	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_tunnel: fix geneve_opt type confusion addition When handling multiple NFTA_TUNNEL_KEY_OPTS_GENEVE attributes, the parsing logic should place every geneve_opt structure one by one compactly. Hence, when deciding the next geneve_opt position, the pointer addition should be in units of char *. However, the current implementation erroneously does type conversion before the addition, which will lead to heap out-of-bounds write. [6.989857] ========== ========== ========== === [6.990293] BUG: KASAN: slab-out-of-bounds in nft_tunnel_obj_init+0x977/0xa70 [6.990725] Write of size 124 at addr ffff888005f18974 by task poc/178	https://git.kernel.org/stable/c/0a93a710d6df334b828ea064c6d39fda34f901dc, https://git.kernel.org/stable/c/1b755d8eb1ace3870789d48fbd94f386ad6e30be, https://git.kernel.org/stable/c/28d88ee1e1cc8ac2d79aeb112717b97c5c833d43	O-LIN-LINU-050525/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[6.991162] [6.991259] CPU: 0 PID: 178 Comm: poc-oob-write Not tainted 6.1.132 #1 [6.991655] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 [6.992281] Call Trace: [6.992423] <TASK> [6.992586] dump_stack_lvl+0x44/0x5c [6.992801] print_report+0x184/0x4be [6.993790] kasan_report+0xc5/0x100 [6.994252] kasan_check_range+0xf3/0x1a0 [6.994486] memcpy+0x38/0x60 [6.994692] nft_tunnel_obj_init+0x977/0xa70 [6.995677] nft_obj_init+0x10c/0x1b0 [6.995891] nf_tables_newobj+0x585/0x950 [6.996922] nfnetlink_rcv_batch+0xdf9/0x1020 [6.998997] nfnetlink_rcv+0x1df/0x220 [6.999537] netlink_unicast+0x395/0x530 [7.000771] netlink_sendmsg+0x3d0/0x6d0 [7.001462] __sock_sendmsg+0x99/0xa0 [7.001707] ____sys_sendmsg+0x409/0x450 [7.002391] ___sys_sendmsg+0xfd/0x170 [7.003145]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__sys_sendmsg+0xea/0x170 [7.004359] do_syscall_64+0x5e/0x90 [7.005817] entry_SYSCALL_64_after_hwframe+0x6e/0xd8 [7.006127] RIP: 0033:0x7ec756d4e407 [7.006339] Code: 48 89 fa 4c 89 df e8 38 aa 00 00 8b 93 08 03 00 00 59 5e 48 83 f8 fc 74 1a 5b c3 0f 1f 84 00 00 00 00 00 48 8b 44 24 10 0f 05 <5b> c3 0f 1f 80 00 00 00 00 00 83 e2 39 83 faf [7.007364] RSP: 002b:00007ffed5d46760 EFLAGS: 00000202 ORIG_RAX: 000000000000002e [7.007827] RAX: ffffffffffffffda RBX: 00007ec756cc4740 RCX: 00007ec756d4e407 [7.008223] RDX: 0000000000000000 RSI: 00007ffed5d467f0 RDI: 0000000000000003 [7.008620] RBP: 00007ffed5d468a0 R08: 0000000000000000 R09: 0000000000000000 [7.009039] R10: 0000000000000000 R11: 0000000000000202 R12: 0000000000000000 [7.009429] R13: 00007ffed5d478b0 R14: 00007ec756ee5000 R15: 00005cbd4e655cb8 Fix this bug with correct pointer addition and conversion in parse and dump code. **CVE ID: CVE-2025-22056**		
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/52a5509ab19a5d3afe301165d9	O-LIN-LINU-050525/330

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ext4: fix OOB read when checking dotdot dir Mounting a corrupted filesystem with directory which contains '.' dir entry with rec_len == block size results in out-of-bounds read (later on, when the corrupted directory is removed). ext4_empty_dir() assumes every ext4 directory contains at least '.' and '..' as directory entries in the first data block. It first loads the '.' dir entry, performs sanity checks by calling ext4_check_dir_entry() and then uses its rec_len member to compute the location of '..' dir entry (in ext4_next_entry). It assumes the '..' dir entry fits into the same data block. If the rec_len of '.' is precisely one block (4KB), it slips through the sanity checks (it is considered the last directory entry in the data block) and leaves "struct ext4_dir_entry_2 *de" point exactly past the memory slot allocated to the data block. The following call to ext4_check_dir_entry() on new value of de then dereferences this pointer which results in out-of-bounds mem access. Fix this by extending __ext4_check_dir_entry() to check for '.' dir entries that reach the end of data block. Make sure to	b5787bba34d842, https://git.kernel.org/stable/c/53bc45da8d8da92ec07877f5922b130562eb4b00, https://git.kernel.org/stable/c/89503e5eae64637d0fa2218912b54660effe7d93	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ignore the phony dir entries for checksum (by checking name_len for non-zero). Note: This is reported by KASAN as use-after-free in case another structure was recently freed from the slot past the bound, but it is really an OOB read. This issue was found by syzkaller tool. Call Trace: [38.594108] BUG: KASAN: slab-use-after-free in __ext4_check_dir_entry+0x67e/0x710 [38.594649] Read of size 2 at addr ffff88802b41a004 by task syz-executor/5375 [38.595158] [38.595288] CPU: 0 UID: 0 PID: 5375 Comm: syz-executor Not tainted 6.14.0-rc7 #1 [38.595298] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [38.595304] Call Trace: [38.595308] <TASK> [38.595311] dump_stack_lvl+0xa7/0xd0 [38.595325] print_address_description.constprop.0+0x2c/0x3f0 [38.595339] ? __ext4_check_dir_entry+0x67e/0x710 [38.595349] print_report+0xaa/0x250 [38.595359] ? __ext4_check_dir_entry+0x67e/0x710 [38.595368] ?		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kasan_addr_to_slab+0x9/0x90 [38.595378] kasan_report+0xab/0xe0 [38.595389] ? __ext4_check_dir_entry+0x67e/0x710 [38.595400] __ext4_check_dir_entry+0x67e/0x710 [38.595410] ext4_empty_dir+0x465/0x990 [38.595421] ? __pfx_ext4_empty_dir+0x10/0x10 [38.595432] ext4_rmdir.part.0+0x29a/0xd10 [38.595441] ? __dquot_initialize+0x2a7/0xbf0 [38.595455] ? __pfx_ext4_rmdir.part.0+0x10/0x10 [38.595464] ? __pfx___dquot_initialize+0x10/0x10 [38.595478] ? down_write+0xdb/0x140 [38.595487] ? __pfx_down_write+0x10/0x10 [38.595497] ext4_rmdir+0xee/0x140 [38.595506] vfs_rmdir+0x209/0x670 [38.595517] ? lookup_one_qstr_excl+0x3b/0x190 [38.595529] do_rmdir+0x363/0x3c0 [38.595537] ? __pfx_do_rmdir+0x10/0x10 [38.595544] ? strncpy_from_user+0x1ff/0x2e0 [38.595561] __x64_sys_unlinkat+0xf0/0x130 [38.595570] do_syscall_64+0x5b/0x180		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[38.595583] entry_SYSCALL_64_after_hwframe+0x76/0x7e **CVE ID: CVE-2025-37785**		
Improper Validation of Array Index	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: clk: samsung: Fix UBSAN panic in samsung_clk_init() With UBSAN_ARRAY_BOUNDS=y, I'm hitting the below panic due to dereferencing `ctx->clk_data.hws` before setting `ctx->clk_data.num = nr_clks`. Move that up to fix the crash. UBSAN: array index out of bounds: 00000000f2005512 [#1] PREEMPT SMP <snip> Call trace: samsung_clk_init+0x110/0x124 (P) samsung_clk_init+0x48/0x124 (L) samsung_cmu_register_one+0x3c/0xa0 exynos_arm64_register_cmu+0x54/0x64 __gs101_cmu_top_of_clk_init_declare+0x28/0x60 ... **CVE ID: CVE-2025-39728**	https://git.kernel.org/stable/c/00307934eb94aaa0a99addfb37b9fe206f945004, https://git.kernel.org/stable/c/0fef48f4a70e45a93e73c39023c3a6ea624714d6, https://git.kernel.org/stable/c/157de9e48007a20c65d02fc0229a16f38134a72d	O-LIN-LINU-050525/331
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0c49f12c77b77a706fd41370c1	O-LIN-LINU-050525/332

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			thermal: int340x: Add NULL check for adev Not all devices have an ACPI companion fwnode, so adev might be NULL. This is similar to the commit cd2fd6eab480 ("platform/x86: int3472: Check for adev == NULL"). Add a check for adev not being set and return -ENODEV in that case to avoid a possible NULL pointer deref in int3402_thermal_probe(). Note, under the same directory, int3400_thermal_probe() has such a check. [rjw: Subject edit, added Fixes:] **CVE ID: CVE-2025-23136**	1910635e491845, https://git.kernel.org/stable/c/2542a3f70e563a9e70e7ded314286535a3321bdb, https://git.kernel.org/stable/c/3155d5261b518776d1b807d9d922669991bbee56	
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netlabel: Fix NULL pointer exception caused by CALIPSO on IPv4 sockets When calling netlbl_conn_setattr(), addr->sa_family is used to determine the function behavior. If sk is an IPv4 socket, but the connect function is called with an IPv6 address, the function calipso_sock_setattr() is triggered. Inside this function, the following code is executed: sk_fullsock(__sk) ?	https://git.kernel.org/stable/c/078aabd567de3d63d37d7673f714e309d369e6e2, https://git.kernel.org/stable/c/172a8a996a337206970467e871dd995ac07640b1, https://git.kernel.org/stable/c/1927d0bcd5b81e80971bf6b8eba267508bd1c78b	O-LIN-LINU-050525/333

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inet_sk(__sk)->pinet6 : NULL; Since sk is an IPv4 socket, pinet6 is NULL, leading to a null pointer dereference. This patch fixes the issue by checking if inet6_sk(sk) returns a NULL pointer before accessing pinet6. **CVE ID: CVE-2025-22063**		
Affected Version(s): From (including) 5.12 Up to (excluding) 5.15.180					
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/vkms: Fix use after free and double free on init error If the driver initialization fails, the vkms_exit() function might access an uninitialized or freed default_config pointer and it might double free it. Fix both possible errors by initializing default_config only when the driver initialization succeeded. **CVE ID: CVE-2025-22097**	https://git.kernel.org/stable/c/1f68f1cf09d06061eb549726ff8339e064eddebd, https://git.kernel.org/stable/c/49a69f67f53518bdd9b7eeebf019a2da6cc0e954, https://git.kernel.org/stable/c/561fc0c5cf41f646f3e9e61784cbc0fc832fb936	O-LIN-LINU-050525/334
Affected Version(s): From (including) 5.13 Up to (excluding) 5.14.19					
Missing Release of Memory after Effective Lifetime	17-Apr-2025	3.3	In the Linux kernel, the following vulnerability has been resolved: can: etas_es58x: es58x_rx_err_msg(): fix memory leak in error path In es58x_rx_err_msg(), if can->do_set_mode() fails, the function directly returns without	https://git.kernel.org/stable/c/4f389e1276a5389c92cef860c9fde8e1c802a871, https://git.kernel.org/stable/c/7eb0881aec26099089f12ae850aebd93190b1dfe, https://git.kern	O-LIN-LINU-050525/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calling netif_rx(skb). This means that the skb previously allocated by alloc_can_err_skb() is not freed. In other terms, this is a memory leak. This patch simply removes the return statement in the error branch and let the function continue. Issue was found with GCC -fanalyzer, please follow the link below for details. **CVE ID: CVE-2021-47671**	el.org/stable/c/d9447f768bc8c60623e4bb3ce65b8f4654d33a50	
Affected Version(s): From (including) 5.13 Up to (excluding) 5.15.180					
NULL Pointer Dereference	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: remoteproc: core: Clear table_sz when rproc_shutdown There is case as below could trigger kernel dump: Use U-Boot to start remote processor(rproc) with resource table published to a fixed address by rproc. After Kernel boots up, stop the rproc, load a new firmware which doesn't have resource table ,and start rproc. When starting rproc with a firmware not have resource table, `memcpy(loaded_table, rproc->cached_table, rproc->table_sz)` will trigger dump, because rproc->cache_table is set to NULL during the last stop operation, but rproc-	https://git.kernel.org/stable/c/068f6648ff5b0c7adeb6c363fae7fb188aa178fa, https://git.kernel.org/stable/c/2df19f5f6f72da6f6ebab7cdb3a3b9f7686bb476, https://git.kernel.org/stable/c/6e66bca8cd51ebedd5d32426906a38e4a3c69c5f	O-LIN-LINU-050525/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>table_sz is still valid. This issue is found on i.MX8MP and i.MX9. Dump as below: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000096000004 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 user pgtable: 4k pages, 48-bit VAs, pgdp=000000010af63000 [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP Modules linked in: CPU: 2 UID: 0 PID: 1060 Comm: sh Not tainted 6.14.0-rc7-next-20250317-dirty #38 Hardware name: NXP i.MX8MPlus EVK board (DT) pstate: a0000005 (NzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __pi_memcpy_generic+0x110/0x22c lr : rproc_start+0x88/0x1e0 Call trace: __pi_memcpy_generic+0x11		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0/0x22c (P) rproc_boot+0x198/0x57c state_store+0x40/0x104 dev_attr_store+0x18/0x2c sysfs_kf_write+0x7c/0x94 kernfs_fop_write_iter+0x120/0x1cc vfs_write+0x240/0x378 ksys_write+0x70/0x108 __arm64_sys_write+0x1c/0x28 invoke_syscall+0x48/0x10c el0_svc_common.constprop.0+0xc0/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x30/0xcc el0t_64_sync_handler+0x10c/0x138 el0t_64_sync+0x198/0x19c Clear rproc->table_sz to address the issue. **CVE ID: CVE-2025-38152**		
Affected Version(s): From (including) 5.15 Up to (excluding) 5.15.3					
Missing Release of Memory after Effective Lifetime	17-Apr-2025	3.3	In the Linux kernel, the following vulnerability has been resolved: can: etas_es58x: es58x_rx_err_msg(): fix memory leak in error path In es58x_rx_err_msg(), if can->do_set_mode() fails, the function directly returns without calling netif_rx(skb). This means that the skb previously allocated by alloc_can_err_skb() is not freed. In other terms, this is a memory leak. This patch simply removes the return statement in the	https://git.kernel.org/stable/c/4f389e1276a5389c92cef860c9fde8e1c802a871, https://git.kernel.org/stable/c/7eb0881aec26099089f12ae850aebd93190b1dfe, https://git.kernel.org/stable/c/d9447f768bc8c60623e4bb3ce65b8f4654d33a50	O-LIN-LINU-050525/337

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			error branch and let the function continue. Issue was found with GCC -fanalyzer, please follow the link below for details. **CVE ID: CVE-2021-47671**		
Affected Version(s): From (including) 5.15.129 Up to (excluding) 5.15.180					

Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved:
			
			tracing: Fix use-after-free in print_graph_function_flags during tracer switching
			
			Kairui reported a UAF issue in print_graph_function_flags() during ftrace stress testing [1]. This issue can be reproduced if puting a 'mdelay(10)' after 'mutex_unlock(&trace_types_lock)' in s_start(), and executing the following script:
			
			$ echo function_graph > current_tracer
			$ cat trace > /dev/null &
			$ sleep 5 # Ensure the 'cat' reaches the 'mdelay(10)' point
			$ echo timerlat > current_tracer
			
			The root cause lies in the two calls to print_graph_function_flags within print_trace_line during each s_show():
			
			* One through 'iter->trace->print_line()';
			* Another through 'event->funcs->trace()', which is hidden in
				https://git.kernel.org/stable/c/099ef3385800828b74933a96c117574637c3fb3a, https://git.kernel.org/stable/c/42561fe62c3628ea3bc9623f64f047605e98857f, https://git.kernel.org/stable/c/70be951bc01e4a0e10d443f3510bb17426f257fb	O-LIN-LINU-050525/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			print_trace_fmt() before print_trace_line returns. Tracer switching only updates the former, while the latter continues to use the print_line function of the old tracer, which in the script above is print_graph_function_flags. Moreover, when switching from the 'function_graph' tracer to the 'timerlat' tracer, s_start only calls graph_trace_close of the 'function_graph' tracer to free 'iter->private', but does not set it to NULL. This provides an opportunity for 'event->funcs->trace()' to use an invalid 'iter->private'. To fix this issue, set 'iter->private' to NULL immediately after freeing it in graph_trace_close(), ensuring that an invalid pointer is not passed to other tracers. Additionally, clean up the unnecessary 'iter->private = NULL' during each 'cat trace' when using wakeup and irqsoff tracers. [1] https://lore.kernel.org/all/20231112150030.84609-1-ryncsn@gmail.com/ **CVE ID: CVE-2025-22035**		
Affected Version(s): From (including) 5.15.143 Up to (excluding) 5.15.180					
NULL Pointer	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has	https://git.kernel.org/stable/c/	O-LIN-LINU-050525/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			been resolved: arcnet: Add NULL check in com20020pci_probe() devm_kasprintf() returns NULL when memory allocation fails. Currently, com20020pci_probe() does not check for this case, which results in a NULL pointer dereference. Add NULL check after devm_kasprintf() to prevent this issue and ensure no resources are left allocated. **CVE ID: CVE-2025-22054**	661cf5d102949898c931e81fd4e1c773afcdeafa, https://git.kernel.org/stable/c/8872261635044494ea7e58033a97c2d2ab12e05d4, https://git.kernel.org/stable/c/905a34dc1ad9a53a8aaaf8a759ea5dbaaa30418d	
Affected Version(s): From (including) 5.15.174 Up to (excluding) 5.15.180					
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: jfs: fix slab-out-of-bounds read in ea_get() During the "size_check" label in ea_get(), the code checks if the extended attribute list (xattr) size matches ea_size. If not, it logs "ea_get: invalid extended attribute" and calls print_hex_dump(). Here, EALIST_SIZE(ea_buf->xattr) returns 4110417968, which exceeds INT_MAX (2,147,483,647). Then ea_size is clamped: int size = clamp_t(int, ea_size, 0, EALIST_SIZE(ea_buf->xattr)); Although clamp_t aims to	https://git.kernel.org/stable/c/0beddc2a3f9b9cf7d8887973041e36c2d0fa3652, https://git.kernel.org/stable/c/16d3d36436492aa248b2d8045e75585ebcc2f34d, https://git.kernel.org/stable/c/3d6fd5b9c6acbc005e53d0211c7381f566babec1	O-LIN-LINU-050525/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			bound ea_size between 0 and 4110417968, the upper limit is treated as an int, causing an overflow above 2^31 - 1. This leads "size" to wrap around and become negative (-184549328).
			
			The "size" is then passed to print_hex_dump() (called "len" in print_hex_dump()), it is passed as type size_t (an unsigned type), this is then stored inside a variable called "int remaining", which is then assigned to "int linelen" which is then passed to hex_dump_to_buffer(). In print_hex_dump() the for loop, iterates through 0 to len-1, where len is 18446744073525002176, calling hex_dump_to_buffer() on each iteration:
			
			for (i = 0; i < len; i += rowsize) {
			linelen = min(remaining, rowsize);
			remaining -= rowsize;
			
			hex_dump_to_buffer (ptr + i, linelen, rowsize, groupsize,
			
			linebuf, sizeof(linebuf), ascii);
			
			...
			}
			
			The expected stopping condition (i < len) is effectively broken		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			since len is corrupted and very large. This eventually leads to the "ptr+i" being passed to hex_dump_to_buffer() to get closer to the end of the actual bounds of "ptr", eventually an out of bounds access is done in hex_dump_to_buffer() in the following for loop:
			
			for (j = 0; j < len; j++) {
			if (linebuflen < lx + 2)
			
			goto overflow2;
			ch = ptr[j];
			...
			}
			
			To fix this we should validate "EALIST_SIZE(ea_buf->xattr)" before it is utilised.
			
			CVE ID: CVE-2025-39735		

Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.134					
Out-of-bounds Write	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_tunnel: fix geneve_opt type confusion addition When handling multiple NFTA_TUNNEL_KEY_OPTS_GENEVE attributes, the parsing logic should place every geneve_opt structure one by one compactly. Hence, when deciding the next geneve_opt position, the pointer addition should be	https://git.kernel.org/stable/c/0a93a710d6df334b828ea064c6d39fda34f901dc, https://git.kernel.org/stable/c/1b755d8eb1ace3870789d48fbd94f386ad6e30be, https://git.kernel.org/stable/c/28d88ee1e1cc8ac2d79aeb112717b97c5c833d43	O-LIN-LINU-050525/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in units of char *. However, the current implementation erroneously does type conversion before the addition, which will lead to heap out-of-bounds write. [6.989857] ========== ========== ========== === [6.990293] BUG: KASAN: slab-out-of-bounds in nft_tunnel_obj_init+0x977/0xa70 [6.990725] Write of size 124 at addr ffff888005f18974 by task poc/178 [6.991162] [6.991259] CPU: 0 PID: 178 Comm: poc-oob-write Not tainted 6.1.132 #1 [6.991655] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 [6.992281] Call Trace: [6.992423] <TASK> [6.992586] dump_stack_lvl+0x44/0x5c [6.992801] print_report+0x184/0x4be [6.993790] kasan_report+0xc5/0x100 [6.994252] kasan_check_range+0xf3/0x1a0 [6.994486] memcpy+0x38/0x60 [6.994692] nft_tunnel_obj_init+0x977/0xa70 [6.995677] nft_obj_init+0x10c/0x1b0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[6.995891] nf_tables_newobj+0x585/0x950 [6.996922] nfnetlink_rcv_batch+0xdf9/0x1020 [6.998997] nfnetlink_rcv+0x1df/0x220 [6.999537] netlink_unicast+0x395/0x530 [7.000771] netlink_sendmsg+0x3d0/0x6d0 [7.001462] __sock_sendmsg+0x99/0xa0 [7.001707] ____sys_sendmsg+0x409/0x450 [7.002391] ___sys_sendmsg+0xfd/0x170 [7.003145] __sys_sendmsg+0xea/0x170 [7.004359] do_syscall_64+0x5e/0x90 [7.005817] entry_SYSCALL_64_after_hwframe+0x6e/0xd8 [7.006127] RIP: 0033:0x7ec756d4e407 [7.006339] Code: 48 89 fa 4c 89 df e8 38 aa 00 00 8b 93 08 03 00 00 59 5e 48 83 f8 fc 74 1a 5b c3 0f 1f 84 00 00 00 00 00 48 8b 44 24 10 0f 05 <5b> c3 0f 1f 80 00 00 00 00 83 e2 39 83 faf [7.007364] RSP: 002b:00007ffed5d46760 EFLAGS: 00000202 ORIG_RAX: 000000000000002e [7.007827] RAX: ffffffffffffffda RBX: 00007ec756cc4740 RCX: 00007ec756d4e407 [7.008223] RDX: 0000000000000000 RSI: 00007ffed5d467f0 RDI: 0000000000000003 [7.008620] RBP:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00007ffed5d468a0 R08: 0000000000000000 R09: 0000000000000000 [7.009039] R10: 0000000000000000 R11: 0000000000000202 R12: 0000000000000000 [7.009429] R13: 00007ffed5d478b0 R14: 00007ec756ee5000 R15: 00005cbd4e655cb8 Fix this bug with correct pointer addition and conversion in parse and dump code. **CVE ID: CVE-2025-22056**		
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/vkms: Fix use after free and double free on init error If the driver initialization fails, the vkms_exit() function might access an uninitialized or freed default_config pointer and it might double free it. Fix both possible errors by initializing default_config only when the driver initialization succeeded. **CVE ID: CVE-2025-22097**	https://git.kernel.org/stable/c/1f68f1cf09d06061eb549726ff8339e064eddebd, https://git.kernel.org/stable/c/49a69f67f53518bdd9b7eeebf019a2da6cc0e954, https://git.kernel.org/stable/c/561fc0c5cf41f646f3e9e61784cbc0fc832fb936	O-LIN-LINU-050525/342
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: ext4: fix OOB read when checking dotdot dir Mounting a corrupted filesystem with directory which contains '.' dir	https://git.kernel.org/stable/c/52a5509ab19a5d3afe301165d9b5787bba34d842, https://git.kernel.org/stable/c/53bc45da8d8da92ec07877f592	O-LIN-LINU-050525/343

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry with rec_len == block size results in out-of-bounds read (later on, when the corrupted directory is removed). ext4_empty_dir() assumes every ext4 directory contains at least '.' and '..' as directory entries in the first data block. It first loads the '.' dir entry, performs sanity checks by calling ext4_check_dir_entry() and then uses its rec_len member to compute the location of '..' dir entry (in ext4_next_entry). It assumes the '..' dir entry fits into the same data block. If the rec_len of '.' is precisely one block (4KB), it slips through the sanity checks (it is considered the last directory entry in the data block) and leaves "struct ext4_dir_entry_2 *de" point exactly past the memory slot allocated to the data block. The following call to ext4_check_dir_entry() on new value of de then dereferences this pointer which results in out-of-bounds mem access. Fix this by extending __ext4_check_dir_entry() to check for '.' dir entries that reach the end of data block. Make sure to ignore the phony dir entries for checksum (by checking name_len for non-zero). Note: This is reported by	2b130562eb4b00, https://git.kernel.org/stable/c/89503e5eae64637d0fa2218912b54660effe7d93	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			KASAN as use-after-free in case another structure was recently freed from the slot past the bound, but it is really an OOB read. This issue was found by syzkaller tool. Call Trace: [38.594108] BUG: KASAN: slab-use-after-free in __ext4_check_dir_entry+0x67e/0x710 [38.594649] Read of size 2 at addr ffff88802b41a004 by task syz-executor/5375 [38.595158] [38.595288] CPU: 0 UID: 0 PID: 5375 Comm: syz-executor Not tainted 6.14.0-rc7 #1 [38.595298] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [38.595304] Call Trace: [38.595308] <TASK> [38.595311] dump_stack_lvl+0xa7/0xd0 [38.595325] print_address_description.constprop.0+0x2c/0x3f0 [38.595339] ? __ext4_check_dir_entry+0x67e/0x710 [38.595349] print_report+0xaa/0x250 [38.595359] ? __ext4_check_dir_entry+0x67e/0x710 [38.595368] ? kasan_addr_to_slab+0x9/0x90 [38.595378] kasan_report+0xab/0xe0 [38.595389] ? __ext4_check_dir_entry+0x6		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7e/0x710 [38.595400] __ext4_check_dir_entry+0x67e/0x710 [38.595410] ext4_empty_dir+0x465/0x990 [38.595421] ? __pfx_ext4_empty_dir+0x10/0x10 [38.595432] ext4_rmdir.part.0+0x29a/0xd10 [38.595441] ? __dquot_initialize+0x2a7/0xbf0 [38.595455] ? __pfx_ext4_rmdir.part.0+0x10/0x10 [38.595464] ? __pfx___dquot_initialize+0x10/0x10 [38.595478] ? down_write+0xdb/0x140 [38.595487] ? __pfx_down_write+0x10/0x10 [38.595497] ext4_rmdir+0xee/0x140 [38.595506] vfs_rmdir+0x209/0x670 [38.595517] ? lookup_one_qstr_excl+0x3b/0x190 [38.595529] do_rmdir+0x363/0x3c0 [38.595537] ? __pfx_do_rmdir+0x10/0x10 [38.595544] ? strncpy_from_user+0x1ff/0x2e0 [38.595561] __x64_sys_unlinkat+0xf0/0x130 [38.595570] do_syscall_64+0x5b/0x180 [38.595583] entry_SYSCALL_64_after_hwframe+0x76/0x7e **CVE ID: CVE-2025-37785**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: remoteproc: core: Clear table_sz when rproc_shutdown There is case as below could trigger kernel dump: Use U-Boot to start remote processor(rproc) with resource table published to a fixed address by rproc. After Kernel boots up, stop the rproc, load a new firmware which doesn't have resource table ,and start rproc. When starting rproc with a firmware not have resource table, `memcpy(loaded_table, rproc->cached_table, rproc->table_sz)` will trigger dump, because rproc->cache_table is set to NULL during the last stop operation, but rproc->table_sz is still valid. This issue is found on i.MX8MP and i.MX9. Dump as below: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000096000004 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000004,	https://git.kernel.org/stable/c/068f6648ff5b0c7adeb6c363fae7fb188aa178fa, https://git.kernel.org/stable/c/2df19f5f6f72da6f6ebab7cdb3a3b9f7686bb476, https://git.kernel.org/stable/c/6e66bca8cd51ebedd5d32426906a38e4a3c69c5f	O-LIN-LINU-050525/344

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 user pgtable: 4k pages, 48-bit VAs, pgdp=000000010af63000 [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP Modules linked in: CPU: 2 UID: 0 PID: 1060 Comm: sh Not tainted 6.14.0-rc7-next-20250317-dirty #38 Hardware name: NXP i.MX8MPlus EVK board (DT) pstate: a0000005 (NzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __pi_memcpy_generic+0x110/0x22c lr : rproc_start+0x88/0x1e0 Call trace: __pi_memcpy_generic+0x110/0x22c (P) rproc_boot+0x198/0x57c state_store+0x40/0x104 dev_attr_store+0x18/0x2c sysfs_kf_write+0x7c/0x94 kernfs_fop_write_iter+0x120/0x1cc vfs_write+0x240/0x378 ksys_write+0x70/0x108 __arm64_sys_write+0x1c/0x28 invoke_syscall+0x48/0x10c el0_svc_common.constprop.0+0xc0/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x30/0xcc el0t_64_sync_handler+0x10		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			c/0x138 el0t_64_sync+0x198/0x19c Clear rproc->table_sz to address the issue. **CVE ID: CVE-2025-38152**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: thermal: int340x: Add NULL check for adev Not all devices have an ACPI companion fwnode, so adev might be NULL. This is similar to the commit cd2fd6eab480 ("platform/x86: int3472: Check for adev == NULL"). Add a check for adev not being set and return -ENODEV in that case to avoid a possible NULL pointer deref in int3402_thermal_probe(). Note, under the same directory, int3400_thermal_probe() has such a check. [rjw: Subject edit, added Fixes:] **CVE ID: CVE-2025-23136**	https://git.kernel.org/stable/c/0c49f12c77b77a706fd41370c11910635e491845, https://git.kernel.org/stable/c/2542a3f70e563a9e70e7ded314286535a3321bdb, https://git.kernel.org/stable/c/3155d5261b518776d1b807d9d922669991bbee56	O-LIN-LINU-050525/345
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netlabel: Fix NULL pointer exception caused by CALIPSO on IPv4 sockets When calling netlbl_conn_setattr(), addr->sa_family is used to determine the function	https://git.kernel.org/stable/c/078aabd567de3d63d37d7673f714e309d369e6e2, https://git.kernel.org/stable/c/172a8a996a337206970467e871dd995ac07640b1,	O-LIN-LINU-050525/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior. If sk is an IPv4 socket, but the connect function is called with an IPv6 address, the function calipso_sock_setattr() is triggered. Inside this function, the following code is executed: sk_fullsock(__sk) ? inet_sk(__sk)->pinet6 : NULL; Since sk is an IPv4 socket, pinet6 is NULL, leading to a null pointer dereference. This patch fixes the issue by checking if inet6_sk(sk) returns a NULL pointer before accessing pinet6. **CVE ID: CVE-2025-22063**	https://git.kernel.org/stable/c/1927d0bcd5b81e80971bf6b8eba267508bd1c78b	
Improper Validation of Array Index	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: clk: samsung: Fix UBSAN panic in samsung_clk_init() With UBSAN_ARRAY_BOUNDS=y, I'm hitting the below panic due to dereferencing `ctx->clk_data.hws` before setting `ctx->clk_data.num = nr_clks`. Move that up to fix the crash. UBSAN: array index out of bounds: 00000000f2005512 [#1] PREEMPT SMP <snip> Call trace: samsung_clk_init+0x110/0x124 (P)	https://git.kernel.org/stable/c/00307934eb94aaa0a99addfb37b9fe206f945004, https://git.kernel.org/stable/c/0fef48f4a70e45a93e73c39023c3a6ea624714d6, https://git.kernel.org/stable/c/157de9e48007a20c65d02fc0229a16f38134a72d	O-LIN-LINU-050525/347

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			samsung_clk_init+0x48/0x124 (L) samsung_cmu_register_one+0x3c/0xa0 exynos_arm64_register_cmu+0x54/0x64 __gs101_cmu_top_of_clk_init_declare+0x28/0x60 ... **CVE ID: CVE-2025-39728**		
Affected Version(s): From (including) 5.4.255 Up to (excluding) 5.4.292					

Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved:
			
			tracing: Fix use-after-free in print_graph_function_flags during tracer switching
			
			Kairui reported a UAF issue in print_graph_function_flags() during ftrace stress testing [1]. This issue can be reproduced if puting a 'mdelay(10)' after 'mutex_unlock(&trace_types_lock)' in s_start(), and executing the following script:
			
			$ echo function_graph > current_tracer
			$ cat trace > /dev/null &
			$ sleep 5 # Ensure the 'cat' reaches the 'mdelay(10)' point
			$ echo timerlat > current_tracer
			
			The root cause lies in the two calls to print_graph_function_flags within print_trace_line during each s_show():
				https://git.kernel.org/stable/c/099ef3385800828b74933a96c117574637c3fb3a, https://git.kernel.org/stable/c/42561fe62c3628ea3bc9623f64f047605e98857f, https://git.kernel.org/stable/c/70be951bc01e4a0e10d443f3510bb17426f257fb	O-LIN-LINU-050525/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* One through 'iter->trace->print_line()'; * Another through 'event->funcs->trace()', which is hidden in print_trace_fmt() before print_trace_line returns. Tracer switching only updates the former, while the latter continues to use the print_line function of the old tracer, which in the script above is print_graph_function_flags. Moreover, when switching from the 'function_graph' tracer to the 'timerlat' tracer, s_start only calls graph_trace_close of the 'function_graph' tracer to free 'iter->private', but does not set it to NULL. This provides an opportunity for 'event->funcs->trace()' to use an invalid 'iter->private'. To fix this issue, set 'iter->private' to NULL immediately after freeing it in graph_trace_close(), ensuring that an invalid pointer is not passed to other tracers. Additionally, clean up the unnecessary 'iter->private = NULL' during each 'cat trace' when using wakeup and irqsoff tracers. [1] https://lore.kernel.org/all/20231112150030.84609-1-ryncsn@gmail.com/		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-22035		
Affected Version(s): From (including) 5.4.264 Up to (excluding) 5.4.292					
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: arcnet: Add NULL check in com20020pci_probe() devm_kasprintf() returns NULL when memory allocation fails. Currently, com20020pci_probe() does not check for this case, which results in a NULL pointer dereference. Add NULL check after devm_kasprintf() to prevent this issue and ensure no resources are left allocated. **CVE ID: CVE-2025-22054**	https://git.kernel.org/stable/c/661cf5d102949898c931e81fd4e1c773afcdeafa, https://git.kernel.org/stable/c/887226163504494ea7e58033a97c2d2ab12e05d4, https://git.kernel.org/stable/c/905a34dc1ad9a53a8aaaf8a759ea5dbaaa30418d	O-LIN-LINU-050525/349
Affected Version(s): From (including) 5.4.287 Up to (excluding) 5.4.292					
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: jfs: fix slab-out-of-bounds read in ea_get() During the "size_check" label in ea_get(), the code checks if the extended attribute list (xattr) size matches ea_size. If not, it logs "ea_get: invalid extended attribute" and calls print_hex_dump(). Here, EALIST_SIZE(ea_buf->xattr) returns 4110417968, which exceeds INT_MAX (2,147,483,647). Then ea_size is clamped:	https://git.kernel.org/stable/c/0beddc2a3f9b9cf7d8887973041e36c2d0fa3652, https://git.kernel.org/stable/c/16d3d36436492aa248b2d8045e75585ebcc2f34d, https://git.kernel.org/stable/c/3d6fd5b9c6acbc005e53d0211c7381f566babec1	O-LIN-LINU-050525/350

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			int size = clamp_t(int, ea_size, 0, EALIST_SIZE(ea_buf->xattr));
			
			Although clamp_t aims to bound ea_size between 0 and 4110417968, the upper limit is treated as an int, causing an overflow above 2^31 - 1. This leads "size" to wrap around and become negative (-184549328).
			
			The "size" is then passed to print_hex_dump() (called "len" in print_hex_dump()), it is passed as type size_t (an unsigned type), this is then stored inside a variable called "int remaining", which is then assigned to "int linelen" which is then passed to hex_dump_to_buffer(). In print_hex_dump() the for loop, iterates through 0 to len-1, where len is 18446744073525002176, calling hex_dump_to_buffer() on each iteration:
			
			for (i = 0; i < len; i += rowsize) {
			linelen = min(remaining, rowsize);
			remaining -= rowsize;
			
			hex_dump_to_buffer (ptr + i, linelen, rowsize, groupsize,
			
			linebuf, sizeof(linebuf), ascii);		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			...
			}
			
			The expected stopping condition (i < len) is effectively broken since len is corrupted and very large. This eventually leads to the "ptr+i" being passed to hex_dump_to_buffer() to get closer to the end of the actual bounds of "ptr", eventually an out of bounds access is done in hex_dump_to_buffer() in the following for loop:
			
			for (j = 0; j < len; j++) {
			if (linebuflen < lx + 2)
			
			goto overflow2;
			ch = ptr[j];
			...
			}
			
			To fix this we should validate "EALIST_SIZE(ea_buf->xattr)" before it is utilised.
			
			CVE ID: CVE-2025-39735		

Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.11					
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_restart: fix use after free bug After calling netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the can_frame cf which aliases skb memory	https://git.kernel.org/stable/c/03f16c5075b22c8902d2af739969e878b0879c94, https://git.kernel.org/stable/c/08ab951787098ae0b6c0364aeea7a8138226f234,	O-LIN-LINU-050525/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is accessed after the netif_rx_ni() in: stats->rx_bytes += cf->len; Reordering the lines solves the issue. **CVE ID: CVE-2021-47668**	https://git.kernel.org/stable/c/260925a0b7d2da5449f8ecfd02c1405e0c8a45b8	
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: peak_usb: fix use after free bugs After calling peak_usb_netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the can_frame cf which aliases skb memory is accessed after the peak_usb_netif_rx_ni(). Reordering the lines solves the issue. **CVE ID: CVE-2021-47670**	https://git.kernel.org/stable/c/50aca891d7a554db0901b245167cd653d73aaa71, https://git.kernel.org/stable/c/5408824636fa0dfedb9ecb0d94abd573131bfbbe, https://git.kernel.org/stable/c/ddd1416f44130377798c1430b76503513b7497c2	O-LIN-LINU-050525/352
Use After Free	17-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: can: vxcan: vxcan_xmit: fix use after free bug After calling netif_rx_ni(skb), dereferencing skb is unsafe. Especially, the canfd_frame cfd which aliases skb memory is accessed after the netif_rx_ni(). **CVE ID: CVE-2021-47669**	https://git.kernel.org/stable/c/6d6dcf2399cdd26f7f5426ca8dd8366b7f2ca105, https://git.kernel.org/stable/c/75854cad5d80976f6ea0f0431f8cedd3bcc475cb, https://git.kernel.org/stable/c/9b820875a32a3443d67bfd368e930383 54e98052	O-LIN-LINU-050525/353
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.236					
Improper Validation of Array Index	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: clk: samsung: Fix UBSAN	https://git.kernel.org/stable/c/00307934eb94aaa0a99addfb37b9fe206f945004	O-LIN-LINU-050525/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			panic in samsung_clk_init() With UBSAN_ARRAY_BOUNDS=y, I'm hitting the below panic due to dereferencing `ctx->clk_data.hws` before setting `ctx->clk_data.num = nr_clks`. Move that up to fix the crash. UBSAN: array index out of bounds: 00000000f2005512 [#1] PREEMPT SMP <snip> Call trace: samsung_clk_init+0x110/0x124 (P) samsung_clk_init+0x48/0x124 (L) samsung_cmu_register_one+0x3c/0xa0 exynos_arm64_register_cmu+0x54/0x64 __gs101_cmu_top_of_clk_init_declare+0x28/0x60 ... **CVE ID: CVE-2025-39728**	, https://git.kernel.org/stable/c/0fef48f4a70e45a93e73c39023c3a6ea624714d6 , https://git.kernel.org/stable/c/157de9e48007a20c65d02fc0229a16f38134a72d	
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netlabel: Fix NULL pointer exception caused by CALIPSO on IPv4 sockets When calling netlbl_conn_setattr(), addr->sa_family is used to determine the function behavior. If sk is an IPv4 socket,	https://git.kernel.org/stable/c/078aabd567de3d63d37d7673f714e309d369e6e2, https://git.kernel.org/stable/c/172a8a996a337206970467e871dd995ac07640b1, https://git.kernel.org/stable/c/	O-LIN-LINU-050525/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			but the connect function is called with an IPv6 address, the function calipso_sock_setattr() is triggered. Inside this function, the following code is executed: sk_fullsock(__sk) ? inet_sk(__sk)->pinet6 : NULL; Since sk is an IPv4 socket, pinet6 is NULL, leading to a null pointer dereference. This patch fixes the issue by checking if inet6_sk(sk) returns a NULL pointer before accessing pinet6. **CVE ID: CVE-2025-22063**	1927d0bcd5b81e80971bf6b8eba267508bd1c78b	
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: thermal: int340x: Add NULL check for adev Not all devices have an ACPI companion fwnode, so adev might be NULL. This is similar to the commit cd2fd6eab480 ("platform/x86: int3472: Check for adev == NULL"). Add a check for adev not being set and return -ENODEV in that case to avoid a possible NULL pointer deref in int3402_thermal_probe(). Note, under the same directory, int3400_thermal_probe() has such a check. [rjw: Subject edit, added	https://git.kernel.org/stable/c/0c49f12c77b77a706fd41370c11910635e491845, https://git.kernel.org/stable/c/2542a3f70e563a9e70e7ded314286535a3321bdb, https://git.kernel.org/stable/c/3155d5261b518776d1b807d9d922669991bbee56	O-LIN-LINU-050525/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fixes:] **CVE ID: CVE-2025-23136**		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.9.9					
NULL Pointer Dereference	17-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: can: dev: can_get_echo_skb(): prevent call to kfree_skb() in hard IRQ context If a driver calls can_get_echo_skb() during a hardware IRQ (which is often, but not always, the case), the 'WARN_ON(in_irq)' in net/core/skbuff.c#skb_release_head_state() might be triggered, under network congestion circumstances, together with the potential risk of a NULL pointer dereference. The root cause of this issue is the call to kfree_skb() instead of dev_kfree_skb_irq() in net/core/dev.c#enqueue_to_backlog(). This patch prevents the skb to be freed within the call to netif_rx() by incrementing its reference count with skb_get(). The skb is finally freed by one of the in-irq-context safe functions: dev_consume_skb_any() or dev_kfree_skb_any(). The "any" version is used because some drivers might call can_get_echo_skb() in a normal context. The reason for this issue to	https://git.kernel.org/stable/c/2283f79b22684d2812e5c76fc2280aae00390365, https://git.kernel.org/stable/c/248b71ce92d4f3a574b2537f9838f48e892618f4, https://git.kernel.org/stable/c/3a922a85701939624484e7f2fd07d32beed00d25	O-LIN-LINU-050525/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occur is that initially, in the core network stack, loopback skb were not supposed to be received in hardware IRQ context. The CAN stack is an exeption. This bug was previously reported back in 2017 in [1] but the proposed patch never got accepted. While [1] directly modifies net/core/dev.c, we try to propose here a smoother modification local to CAN network stack (the assumption behind is that only CAN devices are affected by this issue). [1] http://lore.kernel.org/r/57a3ffb6-3309-3ad5-5a34-e93c3fe3614d@cetitec.com **CVE ID: CVE-2020-36789**		
Affected Version(s): From (including) 5.7 Up to (excluding) 5.10.236					
Out-of-bounds Write	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_tunnel: fix geneve_opt type confusion addition When handling multiple NFTA_TUNNEL_KEY_OPTS_GENEVE attributes, the parsing logic should place every geneve_opt structure one by one compactly. Hence, when deciding the next geneve_opt position, the pointer addition should be in units of char *. However, the current	https://git.kernel.org/stable/c/0a93a710d6df334b828ea064c6d39fda34f901dc, https://git.kernel.org/stable/c/1b755d8eb1ace3870789d48fbd94f386ad6e30be, https://git.kernel.org/stable/c/28d88ee1e1cc8ac2d79aeb112717b97c5c833d43	O-LIN-LINU-050525/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implementation erroneously does type conversion before the addition, which will lead to heap out-of-bounds write. [6.989857] ========== ========== ========== === [6.990293] BUG: KASAN: slab-out-of-bounds in nft_tunnel_obj_init+0x977/0xa70 [6.990725] Write of size 124 at addr ffff888005f18974 by task poc/178 [6.991162] [6.991259] CPU: 0 PID: 178 Comm: poc-oob-write Not tainted 6.1.132 #1 [6.991655] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 [6.992281] Call Trace: [6.992423] <TASK> [6.992586] dump_stack_lvl+0x44/0x5c [6.992801] print_report+0x184/0x4be [6.993790] kasan_report+0xc5/0x100 [6.994252] kasan_check_range+0xf3/0x1a0 [6.994486] memcpy+0x38/0x60 [6.994692] nft_tunnel_obj_init+0x977/0xa70 [6.995677] nft_obj_init+0x10c/0x1b0 [6.995891] nf_tables_newobj+0x585/0x950		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[6.996922] nfnetlink_rcv_batch+0xdf9/0x1020 [6.998997] nfnetlink_rcv+0x1df/0x220 [6.999537] netlink_unicast+0x395/0x530 [7.000771] netlink_sendmsg+0x3d0/0x6d0 [7.001462] __sock_sendmsg+0x99/0xa0 [7.001707] ____sys_sendmsg+0x409/0x450 [7.002391] ___sys_sendmsg+0xfd/0x170 [7.003145] __sys_sendmsg+0xea/0x170 [7.004359] do_syscall_64+0x5e/0x90 [7.005817] entry_SYSCALL_64_after_hwframe+0x6e/0xd8 [7.006127] RIP: 0033:0x7ec756d4e407 [7.006339] Code: 48 89 fa 4c 89 df e8 38 aa 00 00 8b 93 08 03 00 00 59 5e 48 83 f8 fc 74 1a 5b c3 0f 1f 84 00 00 00 00 00 48 8b 44 24 10 0f 05 <5b> c3 0f 1f 80 00 00 00 00 83 e2 39 83 faf [7.007364] RSP: 002b:00007ffed5d46760 EFLAGS: 00000202 ORIG_RAX: 000000000000002e [7.007827] RAX: ffffffffffffffda RBX: 00007ec756cc4740 RCX: 00007ec756d4e407 [7.008223] RDX: 0000000000000000 RSI: 00007ffed5d467f0 RDI: 0000000000000003 [7.008620] RBP: 00007ffed5d468a0 R08: 0000000000000000 R09: 0000000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[7.009039] R10: 0000000000000000 R11: 0000000000000202 R12: 0000000000000000 [7.009429] R13: 00007ffed5d478b0 R14: 00007ec756ee5000 R15: 00005cbd4e655cb8 Fix this bug with correct pointer addition and conversion in parse and dump code. **CVE ID: CVE-2025-22056**		
Affected Version(s): From (including) 6.0 Up to (excluding) 6.1.134					
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/erdma: Prevent use-after-free in erdma_accept_newconn() After the erdma_cep_put(new_cep) being called, new_cep will be freed, and the following dereference will cause a UAF problem. Fix this issue. **CVE ID: CVE-2025-22088**	https://git.kernel.org/stable/c/667a628ab67d359166799fad89b3c6909599558a, https://git.kernel.org/stable/c/78411a133312ce7d8a3239c76a8fd85bca1cc10f, https://git.kernel.org/stable/c/7aa6bb5276d9fec98deb05615a086eeb893854ad	O-LIN-LINU-050525/359
Affected Version(s): From (including) 6.0 Up to (excluding) 6.14.2					
NULL Pointer Dereference	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: sfc: fix NULL dereferences in ef100_process_design_param() Since cited commit, ef100_probe_main() and hence also ef100_check_design_params() run before efx->net_dev is created;	https://git.kernel.org/stable/c/8241ecec1cdc6699ae197d52d58e76bddd995fa5, https://git.kernel.org/stable/c/e56391011381d6d029da377a65ac314cb3d5def2	O-LIN-LINU-050525/360

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consequently, we cannot netif_set_tso_max_size() or _segs() at this point. Move those netif calls to ef100_probe_netdev(), and also replace netif_err within the design params code with pci_err. **CVE ID: CVE-2025-37860**		
Affected Version(s): From (including) 6.1 Up to (excluding) 6.1.134					
Off-by-one Error	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: LoongArch: BPF: Fix off-by-one error in build_prologue() Vincent reported that running BPF progs with tailcalls on LoongArch causes kernel hard lockup. Debugging the issues shows that the JITed image missing a jirl instruction at the end of the epilogue. There are two passes in JIT compiling, the first pass set the flags and the second pass generates JIT code based on those flags. With BPF progs mixing bpf2bpf and tailcalls, build_prologue() generates N insns in the first pass and then generates N+1 insns in the second pass. This makes epilogue_offset off by one and we will jump to some unexpected insn and cause lockup. Fix this by inserting a nop insn. **CVE ID: CVE-2025-37893**	https://git.kernel.org/stable/c/205a2182c51ffebaef54d643e3745e720cded08b, https://git.kernel.org/stable/c/48b904de2408af5f936f0e03f48dfcddeab58aa0, https://git.kernel.org/stable/c/7e2586991e36663c9bc48c828b83eab180ad30a9	O-LIN-LINU-050525/361
NULL Pointer	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has	https://git.kernel.org/stable/c/	O-LIN-LINU-050525/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			been resolved: arm64: Don't call NULL in do_compat_alignment_fixup () do_alignment_t32_to_handler() only fixes up alignment faults for specific instructions; it returns NULL otherwise (e.g. LDREX). When that's the case, signal to the caller that it needs to proceed with the regular alignment fault handling (i.e. SIGBUS). Without this patch, the kernel panics: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000086000006 EC = 0x21: IABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x06: level 2 translation fault user pgtable: 4k pages, 48-bit VAs, pgdp=00000800164aa000 [0000000000000000] pgd=0800081fdbd22003, p4d=0800081fdbd22003, pud=08000815d51c6003, pmd=0000000000000000 Internal error: Oops: 0000000086000006 [#1] SMP Modules linked in: cfg80211 rfkill xt_nat xt_tcpudp xt_conntrack nft_chain_nat xt_MASQUERADE nf_nat nf_conntrack_netlink nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 xfrm_user	2df8ee605eb6806cd41c2095306db05206633a08, https://git.kernel.org/stable/c/617a4b0084a547917669fef2b54253cc9c064990, https://git.kernel.org/stable/c/c28f31deeacda307acfee2f18c0ad904e5123aac	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			xfrm_algo xt_addrtype nft_compat br_netfilter veth nvme_fa> libcrc32c crc32c_generic raid0 multipath linear dm_mod dax raid1 md_mod xhci_pci nvme xhci_hcd nvme_core t10_pi usbcore igb crc64_rocksoft crc64 crc_t10dif crct10dif_generic crct10dif_ce crct10dif_common usb_common i2c_algo_bit i2c> CPU: 2 PID: 3932954 Comm: WPEWebProcess Not tainted 6.1.0-31-arm64 #1 Debian 6.1.128-1 Hardware name: GIGABYTE MP32-AR1-00/MP32-AR1-00, BIOS F18v (SCP: 1.08.20211002) 12/01/2021 pstate: 80400009 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : 0x0 lr : do_compat_alignment_fixup +0xd8/0x3dc sp : ffff80000f973dd0 x29: ffff80000f973dd0 x28: ffff081b42526180 x27: 0000000000000000 x26: 0000000000000000 x25: 0000000000000000 x24: 0000000000000000 x23: 0000000000000004 x22: 0000000000000000 x21: 0000000000000001 x20: 00000000e8551f00 x19: ffff80000f973eb0 x18: 0000000000000000 x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : ffffaebc949bc488		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x8 : 0000000000000000 x7 : 0000000000000000 x6 : 0000000000000000 x5 : 0000000000400000 x4 : 0000ffffffffffe x3 : 0000000000000000 x2 : ffff80000f973eb0 x1 : 00000000e8551f00 x0 : 0000000000000001 Call trace: 0x0 do_alignment_fault+0x40/0x50 do_mem_abort+0x4c/0xa0 el0_da+0x48/0xf0 el0t_32_sync_handler+0x110/0x140 el0t_32_sync+0x190/0x194 Code: bad PC value ---[end trace 0000000000000000]--- **CVE ID: CVE-2025-22033**		
Affected Version(s): From (including) 6.1 Up to (excluding) 6.14.2					
Improper Validation of Array Index	18-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: objtool, spi: amd: Fix out-of-bounds stack access in amd_set_spi_freq() If speed_hz < AMD_SPI_MIN_HZ, amd_set_spi_freq() iterates over the entire amd_spi_freq array without breaking out early, causing 'i' to go beyond the array bounds. Fix that by stopping the loop when it gets to the last entry, so the low speed_hz value gets clamped up to AMD_SPI_MIN_HZ.	https://git.kernel.org/stable/c/76e51db43fe4aaaebcc5ddda67b0807f7c9bdecc, https://git.kernel.org/stable/c/7f2c746e09a3746bf937bc708129dc8af61d8f19	O-LIN-LINU-050525/363

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fixes the following warning with an UBSAN kernel: drivers/spi/spi-amd.o: error: objtool: amd_set_spi_freq() falls through to next function amd_spi_set_opcode() **CVE ID: CVE-2025-40014**		
Affected Version(s): From (including) 6.1.120 Up to (excluding) 6.1.134					
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: jfs: fix slab-out-of-bounds read in ea_get() During the "size_check" label in ea_get(), the code checks if the extended attribute list (xattr) size matches ea_size. If not, it logs "ea_get: invalid extended attribute" and calls print_hex_dump(). Here, EALIST_SIZE(ea_buf->xattr) returns 4110417968, which exceeds INT_MAX (2,147,483,647). Then ea_size is clamped: int size = clamp_t(int, ea_size, 0, EALIST_SIZE(ea_buf->xattr)); Although clamp_t aims to bound ea_size between 0 and 4110417968, the upper limit is treated as an int, causing an overflow above 2^31 - 1. This leads "size" to wrap around and become negative (-184549328).	https://git.kernel.org/stable/c/0beddc2a3f9b9cf7d8887973041e36c2d0fa3652, https://git.kernel.org/stable/c/16d3d36436492aa248b2d8045e75585ebcc2f34d, https://git.kernel.org/stable/c/3d6fd5b9c6acbc005e53d0211c7381f566babec1	O-LIN-LINU-050525/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			The "size" is then passed to print_hex_dump() (called "len" in print_hex_dump()), it is passed as type size_t (an unsigned type), this is then stored inside a variable called "int remaining", which is then assigned to "int linelen" which is then passed to hex_dump_to_buffer(). In print_hex_dump() the for loop, iterates through 0 to len-1, where len is 18446744073525002176, calling hex_dump_to_buffer() on each iteration:
			
			for (i = 0; i < len; i += rowsize) {
			linelen = min(remaining, rowsize);
			remaining -= rowsize;
			
			hex_dump_to_buffer (ptr + i, linelen, rowsize, groupsize,
			
			linebuf, sizeof(linebuf), ascii);
			
			...
			}
			
			The expected stopping condition (i < len) is effectively broken since len is corrupted and very large. This eventually leads to the "ptr+i" being passed to hex_dump_to_buffer() to get closer to the end of the actual bounds of "ptr", eventually an out of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			bounds access is done in hex_dump_to_buffer() in the following for loop:
			
			for (j = 0; j < len; j++) {
			if (linebuflen < lx + 2)
			
			goto overflow2;
			ch = ptr[j];
			...
			}
			
			To fix this we should validate "EALIST_SIZE(ea_buf->xattr)" before it is utilised.
			
			CVE ID: CVE-2025-39735		

Affected Version(s): From (including) 6.1.50 Up to (excluding) 6.1.134					

Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved:
			
			tracing: Fix use-after-free in print_graph_function_flags during tracer switching
			
			Kairui reported a UAF issue in print_graph_function_flags() during ftrace stress testing [1]. This issue can be reproduced if puting a 'mdelay(10)' after 'mutex_unlock(&trace_types_lock)' in s_start(), and executing the following script:
			
			$ echo function_graph > current_tracer
			$ cat trace > /dev/null &
			$ sleep 5 # Ensure the 'cat' reaches the 'mdelay(10)' point
				https://git.kernel.org/stable/c/099ef3385800828b74933a96c117574637c3fb3a, https://git.kernel.org/stable/c/42561fe62c3628ea3bc9623f64f047605e98857f, https://git.kernel.org/stable/c/70be951bc01e4a0e10d443f3510bb17426f257fb	O-LIN-LINU-050525/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			$ echo timerlat > current_tracer The root cause lies in the two calls to print_graph_function_flags within print_trace_line during each s_show(): * One through 'iter->trace->print_line()'; * Another through 'event->funcs->trace()', which is hidden in print_trace_fmt() before print_trace_line returns. Tracer switching only updates the former, while the latter continues to use the print_line function of the old tracer, which in the script above is print_graph_function_flags. Moreover, when switching from the 'function_graph' tracer to the 'timerlat' tracer, s_start only calls graph_trace_close of the 'function_graph' tracer to free 'iter->private', but does not set it to NULL. This provides an opportunity for 'event->funcs->trace()' to use an invalid 'iter->private'. To fix this issue, set 'iter->private' to NULL immediately after freeing it in graph_trace_close(), ensuring that an invalid pointer is not passed to other tracers. Additionally, clean up the unnecessary 'iter->private = NULL'		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during each 'cat trace' when using wakeup and irqsoff tracers. [1] https://lore.kernel.org/all/20231112150030.84609-1-ryncsn@gmail.com/ **CVE ID: CVE-2025-22035**		
Affected Version(s): From (including) 6.1.68 Up to (excluding) 6.1.134					
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: arcnet: Add NULL check in com20020pci_probe() devm_kasprintf() returns NULL when memory allocation fails. Currently, com20020pci_probe() does not check for this case, which results in a NULL pointer dereference. Add NULL check after devm_kasprintf() to prevent this issue and ensure no resources are left allocated. **CVE ID: CVE-2025-22054**	https://git.kernel.org/stable/c/661cf5d102949898c931e81fd4e1c773afcdeafa, https://git.kernel.org/stable/c/8872261635044 94ea7e58033a97c2d2ab12e05d4, https://git.kernel.org/stable/c/905a34dc1ad9a53a8aaaf8a759ea5dbaaa30418d	O-LIN-LINU-050525/366
Affected Version(s): From (including) 6.11 Up to (excluding) 6.12.23					
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: objtool, nvmet: Fix out-of-bounds stack access in nvmet_ctrl_state_show() The csts_state_names[] array only has six sparse entries, but the iteration code in nvmet_ctrl_state_show() iterates seven, resulting in a potential out-of-bounds stack read. Fix that.	https://git.kernel.org/stable/c/0cc0efc58d6c741b2868d4af24874d7fec28a575, https://git.kernel.org/stable/c/107a23185d990e3df6638d9a84c835f963fe30a6, https://git.kernel.org/stable/c/1adc93a525fdee8e2b311e6d5fd93eb69714ca05	O-LIN-LINU-050525/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fixes the following warning with an UBSAN kernel: vmlinux.o: warning: objtool: .text.nvmet_ctrl_state_show: unexpected end of section **CVE ID: CVE-2025-39778**		
Affected Version(s): From (including) 6.11 Up to (excluding) 6.14.2					
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: cpufreq/amd-pstate: Add missing NULL ptr check in amd_pstate_update Check if policy is NULL before dereferencing it in amd_pstate_update. **CVE ID: CVE-2025-23137**	https://git.kernel.org/stable/c/426db24d4db2e4f0d6720aeb7795eafcb9e82640, https://git.kernel.org/stable/c/b99c1c63d88c75a4dc5487c3696cda38697b8d35	O-LIN-LINU-050525/368
Affected Version(s): From (including) 6.11.11 Up to (excluding) 6.12					
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: jfs: fix slab-out-of-bounds read in ea_get() During the "size_check" label in ea_get(), the code checks if the extended attribute list (xattr) size matches ea_size. If not, it logs "ea_get: invalid extended attribute" and calls print_hex_dump(). Here, EALIST_SIZE(ea_buf->xattr) returns 4110417968, which exceeds INT_MAX (2,147,483,647). Then ea_size is clamped: int size =	https://git.kernel.org/stable/c/0beddc2a3f9b9cf7d8887973041e36c2d0fa3652, https://git.kernel.org/stable/c/16d3d36436492aa248b2d8045e75585ebcc2f34d, https://git.kernel.org/stable/c/3d6fd5b9c6acbc005e53d0211c7381f566babec1	O-LIN-LINU-050525/369

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			clamp_t(int, ea_size, 0, EALIST_SIZE(ea_buf->xattr));
			
			Although clamp_t aims to bound ea_size between 0 and 4110417968, the upper limit is treated as an int, causing an overflow above 2^31 - 1. This leads "size" to wrap around and become negative (-184549328).
			
			The "size" is then passed to print_hex_dump() (called "len" in print_hex_dump()), it is passed as type size_t (an unsigned type), this is then stored inside a variable called "int remaining", which is then assigned to "int linelen" which is then passed to hex_dump_to_buffer(). In print_hex_dump() the for loop, iterates through 0 to len-1, where len is 18446744073525002176, calling hex_dump_to_buffer() on each iteration:
			
			for (i = 0; i < len; i += rowsize) {
			linelen = min(remaining, rowsize);
			remaining -= rowsize;
			
			hex_dump_to_buffer (ptr + i, linelen, rowsize, groupsize,
			
			linebuf, sizeof(linebuf), ascii);
			
			...		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			}
			
			The expected stopping condition (i < len) is effectively broken since len is corrupted and very large. This eventually leads to the "ptr+i" being passed to hex_dump_to_buffer() to get closer to the end of the actual bounds of "ptr", eventually an out of bounds access is done in hex_dump_to_buffer() in the following for loop:
			
			for (j = 0; j < len; j++) {
			if (linebuflen < lx + 2)
			
			goto overflow2;
			ch = ptr[j];
			...
			}
			
			To fix this we should validate "EALIST_SIZE(ea_buf->xattr)" before it is utilised.
			
			CVE ID: CVE-2025-39735		

Affected Version(s): From (including) 6.12 Up to (excluding) 6.12.23					
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/core: Fix use-after-free when rename device name Syzbot reported a slab-use-after-free with the following call trace: ==========	https://git.kernel.org/stable/c/0d6460b9d2a3ee380940bdf47680751ef91cb88e, https://git.kernel.org/stable/c/1d6a9e7449e2a0c1e2934eee7880ba8bd1e464cd, https://git.kern	O-LIN-LINU-050525/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			========== ========== === BUG: KASAN: slab-use-after-free in nla_put+0xd3/0x150 lib/nlattr.c:1099 Read of size 5 at addr ffff888140ea1c60 by task syz.0.988/10025 CPU: 0 UID: 0 PID: 10025 Comm: syz.0.988 Not tainted 6.14.0-rc4-syzkaller-00859-gf77f12010f67 #0 Hardware name: Google Compute Engine, BIOS Google 02/12/2025 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:408 [inline] print_report+0x16e/0x5b0 mm/kasan/report.c:521 kasan_report+0x143/0x180 mm/kasan/report.c:634 kasan_check_range+0x282/0x290 mm/kasan/generic.c:189 __asan_memcpy+0x29/0x70 mm/kasan/shadow.c:105 nla_put+0xd3/0x150 lib/nlattr.c:1099 nla_put_string include/net/netlink.h:1621 [inline] fill_nldev_handle+0x16e/0x200 drivers/infiniband/core/nldev.c:265	el.org/stable/c/56ec8580be5174b2b9774066e60f1aad56d201db	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rdma_nl_notify_event+0x561/0xef0 drivers/infiniband/core/nldev.c:2857 ib_device_notify_register+0x22/0x230 drivers/infiniband/core/device.c:1344 ib_register_device+0x1292/0x1460 drivers/infiniband/core/device.c:1460 rxe_register_device+0x233/0x350 drivers/infiniband/sw/rxe/rxe_verbs.c:1540 rxe_net_add+0x74/0xf0 drivers/infiniband/sw/rxe/rxe_net.c:550 rxe_newlink+0xde/0x1a0 drivers/infiniband/sw/rxe/rxe.c:212 nldev_newlink+0x5ea/0x680 drivers/infiniband/core/nldev.c:1795 rdma_nl_rcv_skb drivers/infiniband/core/netlink.c:239 [inline] rdma_nl_rcv+0x6dd/0x9e0 drivers/infiniband/core/netlink.c:259 netlink_unicast_kernel net/netlink/af_netlink.c:1313 [inline] netlink_unicast+0x7f6/0x990 net/netlink/af_netlink.c:1339 netlink_sendmsg+0x8de/0xcb0 net/netlink/af_netlink.c:1883 sock_sendmsg_nosec net/socket.c:709 [inline]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__sock_sendmsg+0x221/0x270 net/socket.c:724 ___sys_sendmsg+0x53a/0x860 net/socket.c:2564 ___sys_sendmsg net/socket.c:2618 [inline] __sys_sendmsg+0x269/0x350 net/socket.c:2650 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f42d1b8d169 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 ... RSP: 002b:00007f42d2960038 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f42d1da6320 RCX: 00007f42d1b8d169 RDX: 0000000000000000 RSI: 00004000000002c0 RDI: 000000000000000c RBP: 00007f42d1c0e2a0 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f42d1da6320 R15: 00007ffe399344a8 </TASK> Allocated by task 10025: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0x98/0xb0 mm/kasan/common.c:394 kasan_kmalloc include/linux/kasan.h:260 [inline] __do_kmalloc_node mm/slub.c:4294 [inline] __kmalloc_node_track_caller_noprof+0x28b/0x4c0 mm/slub.c:4313 __kmemdup_nul mm/util.c:61 [inline] kstrdup+0x42/0x100 mm/util.c:81 kobject_set_name_vargs+0x61/0x120 lib/kobject.c:274 dev_set_name+0xd5/0x120 drivers/base/core.c:3468 assign_name drivers/infiniband/core/device.c:1202 [inline] ib_register_device+0x178/0x1460 drivers/infiniband/core/device.c:1384 rxe_register_device+0x233/0x350 drivers/infiniband/sw/rxe/rxe_verbs.c:1540 rxe_net_add+0x74/0xf0 drivers/infiniband/sw/rxe/rxe_net.c:550 rxe_newlink+0xde/0x1a0 drivers/infiniband/sw/rxe/rxe.c:212 nldev_newlink+0x5ea/0x680 drivers/infiniband/core/nldev.c:1795 rdma_nl_rcv_skb drivers/infiniband/core/netlink.c:239 [inline]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rdma_nl_rcv+0x6dd/0x9e0 drivers/infiniband/core/netlink.c:259 netlink_unicast_kernel net/netlink/af_netlink.c:1313 [inline] netlink_unicast+0x7f6/0x990 net/netlink/af_netlink.c:1339 netlink_sendmsg+0x8de/0xcb0 net ---truncated--- **CVE ID: CVE-2025-22085**		
Affected Version(s): From (including) 6.12.13 Up to (excluding) 6.12.23					
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7921: fix kernel panic due to null pointer dereference Address a kernel panic caused by a null pointer dereference in the `mt792x_rx_get_wcid` function. The issue arises because the `deflink` structure is not properly initialized with the `sta` context. This patch ensures that the `deflink` structure is correctly linked to the `sta` context, preventing the null pointer dereference. BUG: kernel NULL pointer dereference, address: 0000000000000400 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] PREEMPT SMP NOPTI	https://git.kernel.org/stable/c/0cfea60966e4b1239d20bebf02258295e189e82a, https://git.kernel.org/stable/c/5a57f8eb2a17d469d65cd1186cea26b798221d4a, https://git.kernel.org/stable/c/adc3fd2a2277b7cc0b61692463771bf9bd298036	O-LIN-LINU-050525/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU: 0 UID: 0 PID: 470 Comm: mt76-usb-rx phy Not tainted 6.12.13-gentoo-dist #1 Hardware name: /AMD HUDSON-M1, BIOS 4.6.4 11/15/2011 RIP: 0010:mt792x_rx_get_wcid+0x48/0x140 [mt792x_lib] RSP: 0018:ffffa147c055fd98 EFLAGS: 00010202 RAX: 0000000000000000 RBX: ffff8e9ecb652000 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000001 RDI: ffff8e9ecb652000 RBP: 0000000000000685 R08: ffff8e9ec6570000 R09: 0000000000000000 R10: ffff8e9ecd2ca000 R11: ffff8e9f22a217c0 R12: 0000000038010119 R13: 0000000080843801 R14: ffff8e9ec6570000 R15: ffff8e9ecb652000 FS: 0000000000000000(0000) GS:ffff8e9f22a00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000400 CR3: 000000000d2ea000 CR4: 00000000000006f0 Call Trace: <TASK> ? __die_body.cold+0x19/0x27 ? page_fault_oops+0x15a/0x2f0 ? search_module_extables+0x19/0x60 ? search_bpf_extables+0x5f/0x80 ?		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exc_page_fault+0x7e/0x180 ? asm_exc_page_fault+0x26/0x30 ? mt792x_rx_get_wcid+0x48/0x140 [mt792x_lib] mt7921_queue_rx_skb+0x1c6/0xaa0 [mt7921_common] mt76u_alloc_queues+0x784/0x810 [mt76_usb] ? __pfx___mt76_worker_fn+0x10/0x10 [mt76] __mt76_worker_fn+0x4f/0x80 [mt76] kthread+0xd2/0x100 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x34/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> ---[end trace 0000000000000000]--- **CVE ID: CVE-2025-22032**		
Affected Version(s): From (including) 6.12.2 Up to (excluding) 6.12.23					
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: jfs: fix slab-out-of-bounds read in ea_get() During the "size_check" label in ea_get(), the code checks if the extended attribute list (xattr) size matches ea_size. If not, it logs "ea_get: invalid extended attribute" and calls print_hex_dump().	https://git.kernel.org/stable/c/0beddc2a3f9b9cf7d8887973041e36c2d0fa3652, https://git.kernel.org/stable/c/16d3d36436492aa248b2d8045e75585ebcc2f34d, https://git.kernel.org/stable/c/3d6fd5b9c6acbc005e53d0211c7381f566babec1	O-LIN-LINU-050525/372

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			Here, EALIST_SIZE(ea_buf->xattr) returns 4110417968, which exceeds INT_MAX (2,147,483,647). Then ea_size is clamped:
			
			int size = clamp_t(int, ea_size, 0, EALIST_SIZE(ea_buf->xattr));
			
			Although clamp_t aims to bound ea_size between 0 and 4110417968, the upper limit is treated as an int, causing an overflow above 2^31 - 1. This leads "size" to wrap around and become negative (-184549328).
			
			The "size" is then passed to print_hex_dump() (called "len" in print_hex_dump()), it is passed as type size_t (an unsigned type), this is then stored inside a variable called "int remaining", which is then assigned to "int linelen" which is then passed to hex_dump_to_buffer(). In print_hex_dump() the for loop, iterates through 0 to len-1, where len is 18446744073525002176, calling hex_dump_to_buffer() on each iteration:
			
			for (i = 0; i < len; i += rowsize) {
			linelen = min(remaining, rowsize);
			remaining -= rowsize;		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			hex_dump_to_buffer (ptr + i, linelen, rowsize, groupsize,
			
			linebuf, sizeof(linebuf), ascii);
			
			...
			}
			
			The expected stopping condition (i < len) is effectively broken since len is corrupted and very large. This eventually leads to the "ptr+i" being passed to hex_dump_to_buffer() to get closer to the end of the actual bounds of "ptr", eventually an out of bounds access is done in hex_dump_to_buffer() in the following for loop:
			
			for (j = 0; j < len; j++) {
			if (linebuflen < lx + 2)
			
			goto overflow2;
			ch = ptr[j];
			...
			}
			
			To fix this we should validate "EALIST_SIZE(ea_buf->xattr)" before it is utilised.
			
			CVE ID: CVE-2025-39735		

Affected Version(s): From (including) 6.13 Up to (excluding) 6.13.11					
Improper Validation of Array Index	18-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: iio: light: Add check for	https://git.kernel.org/stable/c/18a08b5632809faa671279b3cd27d5f96cc5a3f0,	O-LIN-LINU-050525/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			array bounds in veml6075_read_int_time_ms The array contains only 5 elements, but the index calculated by veml6075_read_int_time_index can range from 0 to 7, which could lead to out-of-bounds access. The check prevents this issue. Coverity Issue CID 1574309: (#1 of 1): Out-of-bounds read (OVERRUN) overrun-local: Overrunning array veml6075_it_ms of 5 4-byte elements at element index 7 (byte offset 31) using index int_index (which evaluates to 7) This is hardening against potentially broken hardware. Good to have but not necessary to backport. **CVE ID: CVE-2025-40114**	https://git.kernel.org/stable/c/7a40b52d4442178bee0cf1c36bc450ab951cef0f, https://git.kernel.org/stable/c/9c40a68b7f97fa487e6c7e67fcf4f846a1f96692	
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in ksmbd_sessions_deregister() In multichannel mode, UAF issue can occur in session_deregister when the second channel sets up a session through the connection of the first channel. session that is freed through the global session table can be accessed again through ->sessions of connection.	https://git.kernel.org/stable/c/15a9605f8d69dc85005b1a00c31a050b8625e1aa, https://git.kernel.org/stable/c/33cc29e221df7a3085ae413e8c26c4e81a151153, https://git.kernel.org/stable/c/8ed0e9d2f410f63525afb8351181eea36c80bcf1	O-LIN-LINU-050525/374

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-22041		

Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved:
			
			tracing: Fix use-after-free in print_graph_function_flags during tracer switching
			
			Kairui reported a UAF issue in print_graph_function_flags() during ftrace stress testing [1]. This issue can be reproduced if puting a 'mdelay(10)' after 'mutex_unlock(&trace_types_lock)' in s_start(), and executing the following script:
			
			$ echo function_graph > current_tracer
			$ cat trace > /dev/null &
			$ sleep 5 # Ensure the 'cat' reaches the 'mdelay(10)' point
			$ echo timerlat > current_tracer
			
			The root cause lies in the two calls to print_graph_function_flags within print_trace_line during each s_show():
			
			* One through 'iter->trace->print_line()';
			* Another through 'event->funcs->trace()', which is hidden in print_trace_fmt() before print_trace_line returns.
			
			Tracer switching only updates the former, while the latter continues to use the print_line function of the old tracer,
				https://git.kernel.org/stable/c/099ef3385800828b74933a96c117574637c3fb3a, https://git.kernel.org/stable/c/42561fe62c3628ea3bc9623f64f047605e98857f, https://git.kernel.org/stable/c/70be951bc01e4a0e10d443f3510bb17426f257fb	O-LIN-LINU-050525/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which in the script above is print_graph_function_flags. Moreover, when switching from the 'function_graph' tracer to the 'timerlat' tracer, s_start only calls graph_trace_close of the 'function_graph' tracer to free 'iter->private', but does not set it to NULL. This provides an opportunity for 'event->funcs->trace()' to use an invalid 'iter->private'. To fix this issue, set 'iter->private' to NULL immediately after freeing it in graph_trace_close(), ensuring that an invalid pointer is not passed to other tracers. Additionally, clean up the unnecessary 'iter->private = NULL' during each 'cat trace' when using wakeup and irqsoff tracers. [1] https://lore.kernel.org/all/20231112150030.84609-1-ryncsn@gmail.com/ **CVE ID: CVE-2025-22035**		
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix session use-after-free in multichannel connection There is a race condition between session setup and ksmbd_sessions_deregister.	https://git.kernel.org/stable/c/3980770cb1470054e6400fd9766866597572673 7, https://git.kernel.org/stable/c/596407adb9af1ee75fe7c7529607783d31b66e7f,	O-LIN-LINU-050525/376

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The session can be freed before the connection is added to channel list of session. This patch check reference count of session before freeing it. **CVE ID: CVE-2025-22040**	https://git.kernel.org/stable/c/7dfbd4c43eed91dd2548a95236908025707a8dfd	
Out-of-bounds Write	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_tunnel: fix geneve_opt type confusion addition When handling multiple NFTA_TUNNEL_KEY_OPTS_GENEVE attributes, the parsing logic should place every geneve_opt structure one by one compactly. Hence, when deciding the next geneve_opt position, the pointer addition should be in units of char *. However, the current implementation erroneously does type conversion before the addition, which will lead to heap out-of-bounds write. [6.989857] ========== ========== ========== === [6.990293] BUG: KASAN: slab-out-of-bounds in nft_tunnel_obj_init+0x977/0xa70 [6.990725] Write of size 124 at addr ffff888005f18974 by task poc/178 [6.991162]	https://git.kernel.org/stable/c/0a93a710d6df334b828ea064c6d39fda34f901dc, https://git.kernel.org/stable/c/1b755d8eb1ace3870789d48fbd94f386ad6e30be, https://git.kernel.org/stable/c/28d88ee1e1cc8ac2d79aeb112717b97c5c833d43	O-LIN-LINU-050525/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[6.991259] CPU: 0 PID: 178 Comm: poc-oob-write Not tainted 6.1.132 #1 [6.991655] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 [6.992281] Call Trace: [6.992423] <TASK> [6.992586] dump_stack_lvl+0x44/0x5c [6.992801] print_report+0x184/0x4be [6.993790] kasan_report+0xc5/0x100 [6.994252] kasan_check_range+0xf3/0x1a0 [6.994486] memcpy+0x38/0x60 [6.994692] nft_tunnel_obj_init+0x977/0xa70 [6.995677] nft_obj_init+0x10c/0x1b0 [6.995891] nf_tables_newobj+0x585/0x950 [6.996922] nfnetlink_rcv_batch+0xdf9/0x1020 [6.998997] nfnetlink_rcv+0x1df/0x220 [6.999537] netlink_unicast+0x395/0x530 [7.000771] netlink_sendmsg+0x3d0/0x6d0 [7.001462] __sock_sendmsg+0x99/0xa0 [7.001707] ____sys_sendmsg+0x409/0x450 [7.002391] ___sys_sendmsg+0xfd/0x170 [7.003145] __sys_sendmsg+0xea/0x170		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[7.004359] do_syscall_64+0x5e/0x90 [7.005817] entry_SYSCALL_64_after_hwframe+0x6e/0xd8 [7.006127] RIP: 0033:0x7ec756d4e407 [7.006339] Code: 48 89 fa 4c 89 df e8 38 aa 00 00 8b 93 08 03 00 00 59 5e 48 83 f8 fc 74 1a 5b c3 0f 1f 84 00 00 00 00 00 48 8b 44 24 10 0f 05 <5b> c3 0f 1f 80 00 00 00 00 83 e2 39 83 faf [7.007364] RSP: 002b:00007ffed5d46760 EFLAGS: 00000202 ORIG_RAX: 000000000000002e [7.007827] RAX: ffffffffffffffda RBX: 00007ec756cc4740 RCX: 00007ec756d4e407 [7.008223] RDX: 0000000000000000 RSI: 00007ffed5d467f0 RDI: 0000000000000003 [7.008620] RBP: 00007ffed5d468a0 R08: 0000000000000000 R09: 0000000000000000 [7.009039] R10: 0000000000000000 R11: 0000000000000202 R12: 0000000000000000 [7.009429] R13: 00007ffed5d478b0 R14: 00007ec756ee5000 R15: 00005cbd4e655cb8 Fix this bug with correct pointer addition and conversion in parse and dump code. **CVE ID: CVE-2025-22056**		
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/core: Fix use-after-	https://git.kernel.org/stable/c/0d6460b9d2a3ee380940bdf47680751ef91cb88	O-LIN-LINU-050525/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			free when rename device name Syzbot reported a slab-use-after-free with the following call trace: ========== ========== ========== === BUG: KASAN: slab-use-after-free in nla_put+0xd3/0x150 lib/nlattr.c:1099 Read of size 5 at addr ffff888140ea1c60 by task syz.0.988/10025 CPU: 0 UID: 0 PID: 10025 Comm: syz.0.988 Not tainted 6.14.0-rc4-syzkaller-00859-gf77f12010f67 #0 Hardware name: Google Compute Engine, BIOS Google 02/12/2025 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:408 [inline] print_report+0x16e/0x5b0 mm/kasan/report.c:521 kasan_report+0x143/0x180 mm/kasan/report.c:634 kasan_check_range+0x282/0x290 mm/kasan/generic.c:189 __asan_memcpy+0x29/0x70 mm/kasan/shadow.c:105 nla_put+0xd3/0x150 lib/nlattr.c:1099 nla_put_string	e, https://git.kernel.org/stable/c/1d6a9e7449e2a0c1e2934eee7880ba8bd1e464cd, https://git.kernel.org/stable/c/56ec8580be5174b2b9774066e60f1aad56d201db	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include/net/netlink.h:1621 [inline] fill_nldev_handle+0x16e/0x200 drivers/infiniband/core/nldev.c:265 rdma_nl_notify_event+0x561/0xef0 drivers/infiniband/core/nldev.c:2857 ib_device_notify_register+0x22/0x230 drivers/infiniband/core/device.c:1344 ib_register_device+0x1292/0x1460 drivers/infiniband/core/device.c:1460 rxe_register_device+0x233/0x350 drivers/infiniband/sw/rxe/rxe_verbs.c:1540 rxe_net_add+0x74/0xf0 drivers/infiniband/sw/rxe/rxe_net.c:550 rxe_newlink+0xde/0x1a0 drivers/infiniband/sw/rxe/rxe.c:212 nldev_newlink+0x5ea/0x680 drivers/infiniband/core/nldev.c:1795 rdma_nl_rcv_skb drivers/infiniband/core/netlink.c:239 [inline] rdma_nl_rcv+0x6dd/0x9e0 drivers/infiniband/core/netlink.c:259 netlink_unicast_kernel net/netlink/af_netlink.c:1313 [inline] netlink_unicast+0x7f6/0x990 net/netlink/af_netlink.c:1339		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netlink_sendmsg+0x8de/0xcb0 net/netlink/af_netlink.c:1883 sock_sendmsg_nosec net/socket.c:709 [inline] __sock_sendmsg+0x221/0x270 net/socket.c:724 ___sys_sendmsg+0x53a/0x860 net/socket.c:2564 ___sys_sendmsg net/socket.c:2618 [inline] __sys_sendmsg+0x269/0x350 net/socket.c:2650 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f42d1b8d169 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 ... RSP: 002b:00007f42d2960038 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f42d1da6320 RCX: 00007f42d1b8d169 RDX: 0000000000000000 RSI: 00004000000002c0 RDI: 000000000000000c RBP: 00007f42d1c0e2a0 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f42d1da6320 R15: 00007ffe399344a8 </TASK>		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Allocated by task 10025: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0x98/0xb0 mm/kasan/common.c:394 kasan_kmalloc include/linux/kasan.h:260 [inline] __do_kmalloc_node mm/slub.c:4294 [inline] __kmalloc_node_track_caller_noprof+0x28b/0x4c0 mm/slub.c:4313 __kmemdup_nul mm/util.c:61 [inline] kstrdup+0x42/0x100 mm/util.c:81 kobject_set_name_vargs+0x61/0x120 lib/kobject.c:274 dev_set_name+0xd5/0x120 drivers/base/core.c:3468 assign_name drivers/infiniband/core/device.c:1202 [inline] ib_register_device+0x178/0x1460 drivers/infiniband/core/device.c:1384 rxe_register_device+0x233/0x350 drivers/infiniband/sw/rxe/rxe_verbs.c:1540 rxe_net_add+0x74/0xf0 drivers/infiniband/sw/rxe/rxe_net.c:550 rxe_newlink+0xde/0x1a0 drivers/infiniband/sw/rxe/rxe.c:212		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nldev_newlink+0x5ea/0x680 drivers/infiniband/core/nldev.c:1795 rdma_nl_rcv_skb drivers/infiniband/core/netlink.c:239 [inline] rdma_nl_rcv+0x6dd/0x9e0 drivers/infiniband/core/netlink.c:259 netlink_unicast_kernel net/netlink/af_netlink.c:1313 [inline] netlink_unicast+0x7f6/0x990 net/netlink/af_netlink.c:1339 netlink_sendmsg+0x8de/0xcb0 net ---truncated--- **CVE ID: CVE-2025-22085**		
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/erdma: Prevent use-after-free in erdma_accept_newconn() After the erdma_cep_put(new_cep) being called, new_cep will be freed, and the following dereference will cause a UAF problem. Fix this issue. **CVE ID: CVE-2025-22088**	https://git.kernel.org/stable/c/667a628ab67d359166799fad89b3c6909599558a, https://git.kernel.org/stable/c/78411a133312ce7d8a3239c76a8fd85bca1cc10f, https://git.kernel.org/stable/c/7aa6bb5276d9fec98deb05615a086eeb893854ad	O-LIN-LINU-050525/379
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/vkms: Fix use after free and double free on init error If the driver initialization	https://git.kernel.org/stable/c/1f68f1cf09d06061eb549726ff8339e064eddebd, https://git.kernel.org/stable/c/49a69f67f53518bdd9b7eeebf01	O-LIN-LINU-050525/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fails, the vkms_exit() function might access an uninitialized or freed default_config pointer and it might double free it. Fix both possible errors by initializing default_config only when the driver initialization succeeded. **CVE ID: CVE-2025-22097**	9a2da6cc0e954, https://git.kernel.org/stable/c/561fc0c5cf41f646f3e9e61784cbc0fc832fb936	
Out-of-bounds Read	16-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate zero num_subauth before sub_auth is accessed Access psid->sub_auth[psid->num_subauth - 1] without checking if num_subauth is non-zero leads to an out-of-bounds read. This patch adds a validation step to ensure num_subauth != 0 before sub_auth is accessed. **CVE ID: CVE-2025-22038**	https://git.kernel.org/stable/c/0e36a3e080d6d8bd7a34e089345d043da4ac8283, https://git.kernel.org/stable/c/3ac65de111c686c95316ade660f8ba7aea3cd3cc, https://git.kernel.org/stable/c/56de7778a48560278c334077ace7b9ac4bfb2fd1	O-LIN-LINU-050525/381
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: jfs: fix slab-out-of-bounds read in ea_get() During the "size_check" label in ea_get(), the code checks if the extended attribute list (xattr) size matches ea_size. If not, it logs "ea_get: invalid extended attribute" and calls print_hex_dump().	https://git.kernel.org/stable/c/0beddc2a3f9b9cf7d8887973041e36c2d0fa3652, https://git.kernel.org/stable/c/16d3d36436492aa248b2d8045e75585ebcc2f34d, https://git.kernel.org/stable/c/3d6fd5b9c6acbc005e53d0211c7381f566babec1	O-LIN-LINU-050525/382

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			Here, EALIST_SIZE(ea_buf->xattr) returns 4110417968, which exceeds INT_MAX (2,147,483,647). Then ea_size is clamped:
			
			int size = clamp_t(int, ea_size, 0, EALIST_SIZE(ea_buf->xattr));
			
			Although clamp_t aims to bound ea_size between 0 and 4110417968, the upper limit is treated as an int, causing an overflow above 2^31 - 1. This leads "size" to wrap around and become negative (-184549328).
			
			The "size" is then passed to print_hex_dump() (called "len" in print_hex_dump()), it is passed as type size_t (an unsigned type), this is then stored inside a variable called "int remaining", which is then assigned to "int linelen" which is then passed to hex_dump_to_buffer(). In print_hex_dump() the for loop, iterates through 0 to len-1, where len is 18446744073525002176, calling hex_dump_to_buffer() on each iteration:
			
			for (i = 0; i < len; i += rowsize) {
			linelen = min(remaining, rowsize);
			remaining -= rowsize;		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			hex_dump_to_buffer (ptr + i, linelen, rowsize, groupsize,
			
			linebuf, sizeof(linebuf), ascii);
			
			...
			}
			
			The expected stopping condition (i < len) is effectively broken since len is corrupted and very large. This eventually leads to the "ptr+i" being passed to hex_dump_to_buffer() to get closer to the end of the actual bounds of "ptr", eventually an out of bounds access is done in hex_dump_to_buffer() in the following for loop:
			
			for (j = 0; j < len; j++) {
			if (linebuflen < lx + 2)
			
			goto overflow2;
			ch = ptr[j];
			...
			}
			
			To fix this we should validate "EALIST_SIZE(ea_buf->xattr)" before it is utilised.
			
			CVE ID: CVE-2025-39735		

Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: objtool, nvmet: Fix out-of-bounds stack access in	https://git.kernel.org/stable/c/0cc0efc58d6c741b2868d4af24874d7fec28a575, https://git.kern	O-LIN-LINU-050525/383

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nvmet_ctrl_state_show() The csts_state_names[] array only has six sparse entries, but the iteration code in nvmet_ctrl_state_show() iterates seven, resulting in a potential out-of-bounds stack read. Fix that. Fixes the following warning with an UBSAN kernel: vmlinux.o: warning: objtool: .text.nvmet_ctrl_state_show: unexpected end of section **CVE ID: CVE-2025-39778**	el.org/stable/c/107a23185d990e3df6638d9a84c835f963fe30a6, https://git.kernel.org/stable/c/1adc93a525fdee8e2b311e6d5fd93eb69714ca05	
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: ext4: fix OOB read when checking dotdot dir Mounting a corrupted filesystem with directory which contains '.' dir entry with rec_len == block size results in out-of-bounds read (later on, when the corrupted directory is removed). ext4_empty_dir() assumes every ext4 directory contains at least '.' and '..' as directory entries in the first data block. It first loads the '.' dir entry, performs sanity checks by calling ext4_check_dir_entry() and then uses its rec_len member to compute the location of '..' dir entry (in ext4_next_entry). It assumes the '..' dir entry fits into the	https://git.kernel.org/stable/c/52a5509ab19a5d3afe301165d9b5787bba34d842, https://git.kernel.org/stable/c/53bc45da8d8da92ec07877f5922b130562eb4b00, https://git.kernel.org/stable/c/89503e5eae64637d0fa2218912b54660effe7d93	O-LIN-LINU-050525/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			same data block. If the rec_len of '.' is precisely one block (4KB), it slips through the sanity checks (it is considered the last directory entry in the data block) and leaves "struct ext4_dir_entry_2 *de" point exactly past the memory slot allocated to the data block. The following call to ext4_check_dir_entry() on new value of de then dereferences this pointer which results in out-of-bounds mem access. Fix this by extending __ext4_check_dir_entry() to check for '.' dir entries that reach the end of data block. Make sure to ignore the phony dir entries for checksum (by checking name_len for non-zero). Note: This is reported by KASAN as use-after-free in case another structure was recently freed from the slot past the bound, but it is really an OOB read. This issue was found by syzkaller tool. Call Trace: [38.594108] BUG: KASAN: slab-use-after-free in __ext4_check_dir_entry+0x67e/0x710 [38.594649] Read of size 2 at addr ffff88802b41a004 by task syz-executor/5375 [38.595158] [38.595288] CPU: 0 UID: 0 PID: 5375 Comm: syz-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executor Not tainted 6.14.0-rc7 #1 [38.595298] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [38.595304] Call Trace: [38.595308] <TASK> [38.595311] dump_stack_lvl+0xa7/0xd0 [38.595325] print_address_description.constprop.0+0x2c/0x3f0 [38.595339] ? __ext4_check_dir_entry+0x67e/0x710 [38.595349] print_report+0xaa/0x250 [38.595359] ? __ext4_check_dir_entry+0x67e/0x710 [38.595368] ? kasan_addr_to_slab+0x9/0x90 [38.595378] kasan_report+0xab/0xe0 [38.595389] ? __ext4_check_dir_entry+0x67e/0x710 [38.595400] __ext4_check_dir_entry+0x67e/0x710 [38.595410] ext4_empty_dir+0x465/0x990 [38.595421] ? __pfx_ext4_empty_dir+0x10/0x10 [38.595432] ext4_rmdir.part.0+0x29a/0xd10 [38.595441] ? __dquot_initialize+0x2a7/0xbf0 [38.595455] ? __pfx_ext4_rmdir.part.0+0x10/0x10 [38.595464] ? __pfx___dquot_initialize+0x1		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0/0x10 [38.595478] ? down_write+0xdb/0x140 [38.595487] ? __pfx_down_write+0x10/0x10 [38.595497] ext4_rmdir+0xee/0x140 [38.595506] vfs_rmdir+0x209/0x670 [38.595517] ? lookup_one_qstr_excl+0x3b/0x190 [38.595529] do_rmdir+0x363/0x3c0 [38.595537] ? __pfx_do_rmdir+0x10/0x10 [38.595544] ? strncpy_from_user+0x1ff/0x2e0 [38.595561] __x64_sys_unlinkat+0xf0/0x130 [38.595570] do_syscall_64+0x5b/0x180 [38.595583] entry_SYSCALL_64_after_hwframe+0x76/0x7e **CVE ID: CVE-2025-37785**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Apr-2025	7	In the Linux kernel, the following vulnerability has been resolved: exfat: fix random stack corruption after get_block When get_block is called with a buffer_head allocated on the stack, such as do_mpage_readpage, stack corruption due to buffer_head UAF may occur in the following race condition situation. <CPU 0> <CPU 1> mpage_read_folio <<bh on stack>>	https://git.kernel.org/stable/c/1bb7ff4204b6d4927e982cd256286c09ed4fd8ca, https://git.kernel.org/stable/c/49b0a6ab8e528a0c1c50e37cef9b9c7c121365f2, https://git.kernel.org/stable/c/f7447286363dc1e410bf30b87d75168f3519f9cc	O-LIN-LINU-050525/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_mpage_readpage exfat_get_block bh_read __bh_read get_bh(bh) submit_bh wait_on_buffer ... end_buffer_read_sync __end_buffer_read_notouch unlock_buffer <<keep going>> ... ... <<bh is not valid out of mpage_read_folio>> . . another_function <<variable A on stack>> put_bh(bh) atomic_dec(bh->b_count) * stack corruption here * This patch returns -EAGAIN if a folio does not have buffers when bh_read needs to be called. By doing this, the caller can fallback to functions like block_read_full_folio(), create a buffer_head in the folio, and then call get_block again. Let's do not call bh_read() with on-stack buffer_head. **CVE ID: CVE-2025-22036**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: PCI/bwctrl: Fix NULL	https://git.kernel.org/stable/c/1181924af78e5299ddec6e457789c02dd596655	O-LIN-LINU-050525/386

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pointer dereference on bus number exhaustion When BIOS neglects to assign bus numbers to PCI bridges, the kernel attempts to correct that during PCI device enumeration. If it runs out of bus numbers, no pci_bus is allocated and the "subordinate" pointer in the bridge's pci_dev remains NULL. The PCIe bandwidth controller erroneously does not check for a NULL subordinate pointer and dereferences it on probe. Bandwidth control of unusable devices below the bridge is of questionable utility, so simply error out instead. This mirrors what PCIe hotplug does since commit 62e4492c3063 ("PCI: Prevent NULL dereference during pciehp probe"). The PCI core emits a message with KERN_INFO severity if it has run out of bus numbers. PCIe hotplug emits an additional message with KERN_ERR severity to inform the user that hotplug functionality is disabled at the bridge. A similar message for bandwidth control does not seem merited, given that its only purpose so far is to expose an up-to-date link speed in sysfs and throttle the link speed on certain laptops with limited Thermal Design Power. So	9, https://git.kernel.org/stable/c/667f053b05f00a007738cd7ed6fa1901de19dc7e, https://git.kernel.org/stable/c/d93d309013e89631630a12b1770d27e4be78362a	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			error out silently. User-visible messages: pci 0000:16:02.0: bridge configuration invalid ([bus 00-00]), reconfiguring [...] pci_bus 0000:45: busn_res: [bus 45-74] end is updated to 74 pci 0000:16:02.0: devices behind bridge are unusable because [bus 45-74] cannot be assigned for them [...] pcieport 0000:16:02.0: pciehp: Hotplug bridge without secondary bus, ignoring [...] BUG: kernel NULL pointer dereference RIP: pcie_update_link_speed pcie_bwnotif_enable pcie_bwnotif_probe pcie_port_probe_service really_probe **CVE ID: CVE-2025-22031**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: staging: gpib: Fix Oops after disconnect in ni_usb If the usb dongle is disconnected subsequent calls to the driver cause a NULL dereference Oops as the bus_interface is set to NULL on disconnect. This problem was introduced by setting usb_dev from the bus_interface	https://git.kernel.org/stable/c/5dc98ba6f7304c188b267ef481281849638447bf, https://git.kernel.org/stable/c/a239c6e91b665f1837cf57b97fe638ef1baf2e78, https://git.kernel.org/stable/c/b2d8d7959077c5d4b11d0dc6bd2167791fd1c72e	O-LIN-LINU-050525/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for dev_xxx messages. Previously bus_interface was checked for NULL only in the the functions directly calling usb_fill_bulk_urb or usb_control_msg. Check for valid bus_interface on all interface entry points and return -ENODEV if it is NULL. **CVE ID: CVE-2025-22052**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: arcnet: Add NULL check in com20020pci_probe() devm_kasprintf() returns NULL when memory allocation fails. Currently, com20020pci_probe() does not check for this case, which results in a NULL pointer dereference. Add NULL check after devm_kasprintf() to prevent this issue and ensure no resources are left allocated. **CVE ID: CVE-2025-22054**	https://git.kernel.org/stable/c/661cf5d102949898c931e81fd4e1c773afcdeafa, https://git.kernel.org/stable/c/887226163504494ea7e58033a97c2d2ab12e05d4, https://git.kernel.org/stable/c/905a34dc1ad9a53a8aaaf8a759ea5dbaaa30418d	O-LIN-LINU-050525/388
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: arm64: Don't call NULL in do_compat_alignment_fixup() do_alignment_t32_to_handler() only fixes up alignment faults for specific instructions; it returns NULL otherwise	https://git.kernel.org/stable/c/2df8ee605eb6806cd41c2095306db05206633a08, https://git.kernel.org/stable/c/617a4b0084a547917669fef2b54253cc9c064990, https://git.kernel.org/stable/c/	O-LIN-LINU-050525/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(e.g. LDREX). When that's the case, signal to the caller that it needs to proceed with the regular alignment fault handling (i.e. SIGBUS). Without this patch, the kernel panics: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000086000006 EC = 0x21: IABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x06: level 2 translation fault user pgtable: 4k pages, 48-bit VAs, pgdp=00000800164aa000 [0000000000000000] pgd=0800081fdbd22003, p4d=0800081fdbd22003, pud=08000815d51c6003, pmd=0000000000000000 Internal error: Oops: 0000000086000006 [#1] SMP Modules linked in: cfg80211 rfkill xt_nat xt_tcpudp xt_conntrack nft_chain_nat xt_MASQUERADE nf_nat nf_conntrack_netlink nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 xfrm_user xfrm_algo xt_addrtype nft_compat br_netfilter veth nvme_fa> libcrc32c crc32c_generic raid0 multipath linear dm_mod dax raid1 md_mod xhci_pci nvme xhci_hcd nvme_core t10_pi usbcore igb crc64_rocksoft crc64 crc_t10dif crct10dif_generic crct10dif_ce	c28f31deeacda307acfee2f18c0ad904e5123aac	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crct10dif_common usb_common i2c_algo_bit i2c> CPU: 2 PID: 3932954 Comm: WPEWebProcess Not tainted 6.1.0-31-arm64 #1 Debian 6.1.128-1 Hardware name: GIGABYTE MP32-AR1-00/MP32-AR1-00, BIOS F18v (SCP: 1.08.20211002) 12/01/2021 pstate: 80400009 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : 0x0 lr : do_compat_alignment_fixup +0xd8/0x3dc sp : ffff80000f973dd0 x29: ffff80000f973dd0 x28: ffff081b42526180 x27: 0000000000000000 x26: 0000000000000000 x25: 0000000000000000 x24: 0000000000000000 x23: 0000000000000004 x22: 0000000000000000 x21: 0000000000000001 x20: 00000000e8551f00 x19: ffff80000f973eb0 x18: 0000000000000000 x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : ffffaebc949bc488 x8 : 0000000000000000 x7 : 0000000000000000 x6 : 0000000000000000 x5 : 0000000000400000 x4 : 0000fffffffffffe x3 : 0000000000000000 x2 : ffff80000f973eb0 x1 : 00000000e8551f00 x0 : 0000000000000001 Call trace: 0x0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_alignment_fault+0x40/0x50 do_mem_abort+0x4c/0xa0 el0_da+0x48/0xf0 el0t_32_sync_handler+0x110/0x140 el0t_32_sync+0x190/0x194 Code: bad PC value ---[end trace 0000000000000000]--- **CVE ID: CVE-2025-22033**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix null pointer dereference in alloc_preauth_hash() The Client send malformed smb2 negotiate request. ksmbd return error response. Subsequently, the client can send smb2 session setup even thought conn->preauth_info is not allocated. This patch add KSMBD_SESS_NEED_SETUP status of connection to ignore session setup request if smb2 negotiate phase is not complete. **CVE ID: CVE-2025-22037**	https://git.kernel.org/stable/c/8f216b33a5e1b3489c073b1ea1b3d7cb63c8dc4d, https://git.kernel.org/stable/c/b8eb243e670ecf30e91524dd12f7260dac07d335, https://git.kernel.org/stable/c/c8b5b7c5da7d0c31c9b7190b4a7bba5281fc4780	O-LIN-LINU-050525/390
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: staging: gpib: Fix Oops after disconnect in agilent usb If the agilent usb dongle is disconnected subsequent calls to the	https://git.kernel.org/stable/c/50ef6e45bec79da4c5a01fad4dc23466ba255099, https://git.kernel.org/stable/c/8491e73a5223acb0a4b4d78c3f8b96aa9c5e774d,	O-LIN-LINU-050525/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver cause a NULL dereference Oops as the bus_interface is set to NULL on disconnect. This problem was introduced by setting usb_dev from the bus_interface for dev_xxx messages. Previously bus_interface was checked for NULL only in the functions directly calling usb_fill_bulk_urb or usb_control_msg. Check for valid bus_interface on all interface entry points and return -ENODEV if it is NULL. **CVE ID: CVE-2025-22051**	https://git.kernel.org/stable/c/e88633705078f40391a9afc6cc8ea3025e6f692b	
Off-by-one Error	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: LoongArch: BPF: Fix off-by-one error in build_prologue() Vincent reported that running BPF progs with tailcalls on LoongArch causes kernel hard lockup. Debugging the issues shows that the JITed image missing a jirl instruction at the end of the epilogue. There are two passes in JIT compiling, the first pass set the flags and the second pass generates JIT code based on those flags. With BPF progs mixing bpf2bpf and tailcalls,	https://git.kernel.org/stable/c/205a2182c51ffebaef54d643e3745e720cded08b, https://git.kernel.org/stable/c/48b904de2408af5f936f0e03f48dfcddeab58aa0, https://git.kernel.org/stable/c/7e2586991e36663c9bc48c828b83eab180ad30a9	O-LIN-LINU-050525/392

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			build_prologue() generates N insns in the first pass and then generates N+1 insns in the second pass. This makes epilogue_offset off by one and we will jump to some unexpected insn and cause lockup. Fix this by inserting a nop insn. **CVE ID: CVE-2025-37893**		
NULL Pointer Dereference	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: x86/resctrl: Fix allocation of cleanest CLOSID on platforms with no monitors Commit 6eac36bb9eb0 ("x86/resctrl: Allocate the cleanest CLOSID by searching closid_num_dirty_rmid") added logic that causes resctrl to search for the CLOSID with the fewest dirty cache lines when creating a new control group, if requested by the arch code. This depends on the values read from the llc_occupancy counters. The logic is applicable to architectures where the CLOSID effectively forms part of the monitoring identifier and so do not allow complete freedom to choose an unused monitoring identifier for a given CLOSID. This support missed that some platforms may not have these counters. This	https://git.kernel.org/stable/c/93a418fc61da13d1ee4047d4d1327990f7a2816a, https://git.kernel.org/stable/c/a121798ae669351ec0697c94f71c3a692b2a755b, https://git.kernel.org/stable/c/a8a1bcc27d4607227088d80483164289b5348293	O-LIN-LINU-050525/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causes a NULL pointer dereference when creating a new control group as the array was not allocated by dom_data_init(). As this feature isn't necessary on platforms that don't have cache occupancy monitors, add this to the check that occurs when a new control group is allocated. **CVE ID: CVE-2025-38049**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netlabel: Fix NULL pointer exception caused by CALIPSO on IPv4 sockets When calling netlbl_conn_setattr(), addr->sa_family is used to determine the function behavior. If sk is an IPv4 socket, but the connect function is called with an IPv6 address, the function calipso_sock_setattr() is triggered. Inside this function, the following code is executed: sk_fullsock(__sk) ? inet_sk(__sk)->pinet6 : NULL; Since sk is an IPv4 socket, pinet6 is NULL, leading to a null pointer dereference. This patch fixes the issue by checking if inet6_sk(sk) returns a NULL pointer before accessing pinet6. **CVE ID: CVE-2025-22063**	https://git.kernel.org/stable/c/078aabd567de3d63d37d7673f714e309d369e6e2, https://git.kernel.org/stable/c/172a8a996a337206970467e871dd995ac07640b1, https://git.kernel.org/stable/c/1927d0bcd5b81e80971bf6b8eba267508bd1c78b	O-LIN-LINU-050525/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Locking	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: ALSA: timer: Don't take register_mutex with copy_from/to_user() The infamous mmap_lock taken in copy_from/to_user() can be often problematic when it's called inside another mutex, as they might lead to deadlocks. In the case of ALSA timer code, the bad pattern is with guard(mutex)(&register_mutex) that covers copy_from/to_user() -- which was mistakenly introduced at converting to guard(), and it had been carefully worked around in the past. This patch fixes those pieces simply by moving copy_from/to_user() out of the register mutex lock again. **CVE ID: CVE-2025-23134**	https://git.kernel.org/stable/c/15291b561d8cc835a2eea76b394070cf8e072771, https://git.kernel.org/stable/c/296f7a9e15aab276db11206cbc1e2ae1215d7862, https://git.kernel.org/stable/c/3424c8f53bc63c87712a7fc22dc13d0cc85fb0d6	O-LIN-LINU-050525/395
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: thermal: int340x: Add NULL check for adev Not all devices have an ACPI companion fwnode, so adev might be NULL. This is similar to the commit cd2fd6eab480 ("platform/x86: int3472: Check for adev == NULL").	https://git.kernel.org/stable/c/0c49f12c77b77a706fd41370c11910635e491845, https://git.kernel.org/stable/c/2542a3f70e563a9e70e7ded314286535a3321bdb, https://git.kernel.org/stable/c/	O-LIN-LINU-050525/396

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Add a check for adev not being set and return -ENODEV in that case to avoid a possible NULL pointer deref in int3402_thermal_probe(). Note, under the same directory, int3400_thermal_probe() has such a check. [rjw: Subject edit, added Fixes:] **CVE ID: CVE-2025-23136**	3155d5261b518776d1b807d9d922669991bbee56	
NULL Pointer Dereference	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: remoteproc: core: Clear table_sz when rproc_shutdown There is case as below could trigger kernel dump: Use U-Boot to start remote processor(rproc) with resource table published to a fixed address by rproc. After Kernel boots up, stop the rproc, load a new firmware which doesn't have resource table ,and start rproc. When starting rproc with a firmware not have resource table, `memcpy(loaded_table, rproc->cached_table, rproc->table_sz)` will trigger dump, because rproc->cache_table is set to NULL during the last stop operation, but rproc->table_sz is still valid.	https://git.kernel.org/stable/c/068f6648ff5b0c7adeb6c363fae7fb188aa178fa, https://git.kernel.org/stable/c/2df19f5f6f72da6f6ebab7cdb3a3b9f7686bb476, https://git.kernel.org/stable/c/6e66bca8cd51ebedd5d32426906a38e4a3c69c5f	O-LIN-LINU-050525/397

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue is found on i.MX8MP and i.MX9. Dump as below: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000096000004 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 user pgtable: 4k pages, 48-bit VAs, pgdp=000000010af63000 [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP Modules linked in: CPU: 2 UID: 0 PID: 1060 Comm: sh Not tainted 6.14.0-rc7-next-20250317-dirty #38 Hardware name: NXP i.MX8MPlus EVK board (DT) pstate: a0000005 (NzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __pi_memcpy_generic+0x110/0x22c lr : rproc_start+0x88/0x1e0 Call trace: __pi_memcpy_generic+0x110/0x22c (P) rproc_boot+0x198/0x57c		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			state_store+0x40/0x104 dev_attr_store+0x18/0x2c sysfs_kf_write+0x7c/0x94 kernfs_fop_write_iter+0x120/0x1cc vfs_write+0x240/0x378 ksys_write+0x70/0x108 __arm64_sys_write+0x1c/0x28 invoke_syscall+0x48/0x10c el0_svc_common.constprop.0+0xc0/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x30/0xcc el0t_64_sync_handler+0x10c/0x138 el0t_64_sync+0x198/0x19c Clear rproc->table_sz to address the issue. **CVE ID: CVE-2025-38152**		
Improper Validation of Array Index	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: clk: samsung: Fix UBSAN panic in samsung_clk_init() With UBSAN_ARRAY_BOUNDS=y, I'm hitting the below panic due to dereferencing `ctx->clk_data.hws` before setting `ctx->clk_data.num = nr_clks`. Move that up to fix the crash. UBSAN: array index out of bounds: 00000000f2005512 [#1] PREEMPT SMP <snip> Call trace:	https://git.kernel.org/stable/c/00307934eb94aaa0a99addfb37b9fe206f945004, https://git.kernel.org/stable/c/0fef48f4a70e45a93e73c39023c3a6ea624714d6, https://git.kernel.org/stable/c/157de9e48007a20c65d02fc0229a16f38134a72d	O-LIN-LINU-050525/398

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			samsung_clk_init+0x110/0x124 (P) samsung_clk_init+0x48/0x124 (L) samsung_cmu_register_one+0x3c/0xa0 exynos_arm64_register_cmu+0x54/0x64 __gs101_cmu_top_of_clk_init_declare+0x28/0x60 ... **CVE ID: CVE-2025-39728**		
NULL Pointer Dereference	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: staging: gpib: Fix cb7210 pcmcia Oops The pcmcia_driver struct was still only using the old .name initialization in the drv field. This led to a NULL pointer deref Oops in strcmp called from pcmcia_register_driver. Initialize the pcmcia_driver struct name field. **CVE ID: CVE-2025-39755**	https://git.kernel.org/stable/c/7ec50077d7f6647cb6ba3a2a20a6c26f51259c7d, https://git.kernel.org/stable/c/c1baf6528bcfd6a86842093ff3f8ff8caf309c12, https://git.kernel.org/stable/c/c82ae06f49e70d1c14ee9c76c392345856d050c9	O-LIN-LINU-050525/399
Affected Version(s): From (including) 6.13 Up to (excluding) 6.13.12					
Use After Free	18-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: HSI: ssi_protocol: Fix use after free vulnerability in ssi_protocol Driver Due to Race Condition In the ssi_protocol_probe() function, &ssi->work is bound with ssip_xmit_work(), In	https://git.kernel.org/stable/c/4b4194c9a7a8f92db39e8e86c85f4fb12ebbec4f, https://git.kernel.org/stable/c/58eb29dba712ab0f13af59ca2fe545f5ce360e78, https://git.kernel.org/stable/c/834e602d0cc7c	O-LIN-LINU-050525/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ssip_pn_setup(), the ssip_pn_xmit() function within the ssip_pn_ops structure is capable of starting the work. If we remove the module which will call ssi_protocol_remove() to make a cleanup, it will free ssi through kfree(ssi), while the work mentioned above will be used. The sequence of operations that may lead to a UAF bug is as follows: CPU0 CPU1 | ssip_xmit_work ssi_protocol_remove | kfree(ssi); | | struct hsi_client *cl = ssi->cl; | // use ssi Fix it by ensuring that the work is canceled before proceeding with the cleanup in ssi_protocol_remove(). **CVE ID: CVE-2025-37838**	743bfce734fad4a46cefc0f9ab1	
Affected Version(s): From (including) 6.13.2 Up to (excluding) 6.13.11					
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7921: fix kernel panic due to null pointer dereference Address a kernel panic caused by a null pointer dereference in the `mt792x_rx_get_wcid` function. The issue arises because the `deflink`	https://git.kernel.org/stable/c/0cfea60966e4b1239d20bebf02258295e189e82a, https://git.kernel.org/stable/c/5a57f8eb2a17d469d65cd1186cea26b798221d4a, https://git.kernel.org/stable/c/	O-LIN-LINU-050525/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			structure is not properly initialized with the `sta` context. This patch ensures that the `deflink` structure is correctly linked to the `sta` context, preventing the null pointer dereference. BUG: kernel NULL pointer dereference, address: 0000000000000400 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 0 UID: 0 PID: 470 Comm: mt76-usb-rx phy Not tainted 6.12.13-gentoo-dist #1 Hardware name: /AMD HUDSON-M1, BIOS 4.6.4 11/15/2011 RIP: 0010:mt792x_rx_get_wcid+0x48/0x140 [mt792x_lib] RSP: 0018:ffffa147c055fd98 EFLAGS: 00010202 RAX: 0000000000000000 RBX: ffff8e9ecb652000 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000001 RDI: ffff8e9ecb652000 RBP: 0000000000000685 R08: ffff8e9ec6570000 R09: 0000000000000000 R10: ffff8e9ecd2ca000 R11: ffff8e9f22a217c0 R12: 0000000038010119 R13: 0000000080843801 R14: ffff8e9ec6570000 R15: ffff8e9ecb652000 FS: 0000000000000000(0000) GS:ffff8e9f22a00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES:	adc3fd2a2277b7cc0b61692463771bf9bd298036	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000 CR0: 0000000080050033 CR2: 0000000000000400 CR3: 000000000d2ea000 CR4: 00000000000006f0 Call Trace: <TASK> ? __die_body.cold+0x19/0x27 ? page_fault_oops+0x15a/0x2f0 ? search_module_extables+0x19/0x60 ? search_bpf_extables+0x5f/0x80 ? exc_page_fault+0x7e/0x180 ? asm_exc_page_fault+0x26/0x30 ? mt792x_rx_get_wcid+0x48/0x140 [mt792x_lib] mt7921_queue_rx_skb+0x1c6/0xaa0 [mt7921_common] mt76u_alloc_queues+0x784/0x810 [mt76_usb] ? __pfx___mt76_worker_fn+0x10/0x10 [mt76] __mt76_worker_fn+0x4f/0x80 [mt76] kthread+0xd2/0x100 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x34/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> ---[end trace 0000000000000000]--- **CVE ID: CVE-2025-22032**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 6.14 Up to (excluding) 6.14.2					

Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved:
			
			tracing: Fix use-after-free in print_graph_function_flags during tracer switching
			
			Kairui reported a UAF issue in print_graph_function_flags() during ftrace stress testing [1]. This issue can be reproduced if puting a 'mdelay(10)' after 'mutex_unlock(&trace_types_lock)' in s_start(), and executing the following script:
			
			$ echo function_graph > current_tracer
			$ cat trace > /dev/null &
			$ sleep 5 # Ensure the 'cat' reaches the 'mdelay(10)' point
			$ echo timerlat > current_tracer
			
			The root cause lies in the two calls to print_graph_function_flags within print_trace_line during each s_show():
			
			* One through 'iter->trace->print_line()';
			* Another through 'event->funcs->trace()', which is hidden in print_trace_fmt() before print_trace_line returns.
			
			Tracer switching only updates the former, while the latter continues to use the print_line function of the old tracer, which in the script
				https://git.kernel.org/stable/c/099ef3385800828b74933a96c117574637c3fb3a, https://git.kernel.org/stable/c/42561fe62c3628ea3bc9623f64f047605e98857f, https://git.kernel.org/stable/c/70be951bc01e4a0e10d443f3510bb17426f257fb	O-LIN-LINU-050525/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			above is print_graph_function_flags. Moreover, when switching from the 'function_graph' tracer to the 'timerlat' tracer, s_start only calls graph_trace_close of the 'function_graph' tracer to free 'iter->private', but does not set it to NULL. This provides an opportunity for 'event->funcs->trace()' to use an invalid 'iter->private'. To fix this issue, set 'iter->private' to NULL immediately after freeing it in graph_trace_close(), ensuring that an invalid pointer is not passed to other tracers. Additionally, clean up the unnecessary 'iter->private = NULL' during each 'cat trace' when using wakeup and irqsoff tracers. [1] https://lore.kernel.org/all/20231112150030.84609-1-ryncsn@gmail.com/ **CVE ID: CVE-2025-22035**		
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix session use-after-free in multichannel connection There is a race condition between session setup and ksmbd_sessions_deregister. The session can be freed	https://git.kernel.org/stable/c/3980770cb1470054e6400fd9766866597572673 7, https://git.kernel.org/stable/c/596407adb9af1ee75fe7c7529607783d31b66e7f, https://git.kern	O-LIN-LINU-050525/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before the connection is added to channel list of session. This patch check reference count of session before freeing it. **CVE ID: CVE-2025-22040**	el.org/stable/c/7dfbd4c43eed91dd2548a95236908025707a8dfd	
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in ksmbd_sessions_deregister() In multichannel mode, UAF issue can occur in session_deregister when the second channel sets up a session through the connection of the first channel. session that is freed through the global session table can be accessed again through ->sessions of connection. **CVE ID: CVE-2025-22041**	https://git.kernel.org/stable/c/15a9605f8d69dc85005b1a00c31a050b8625e1aa, https://git.kernel.org/stable/c/33cc29e221df7a3085ae413e8c26c4e81a151153, https://git.kernel.org/stable/c/8ed0e9d2f410f63525afb8351181eea36c80bcf1	O-LIN-LINU-050525/404
Improper Validation of Array Index	18-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: iio: light: Add check for array bounds in veml6075_read_int_time_ms The array contains only 5 elements, but the index calculated by veml6075_read_int_time_index can range from 0 to 7, which could lead to out-of-bounds access. The check prevents this issue. Coverity Issue CID 1574309: (#1 of 1): Out-of-bounds read (OVERRUN)	https://git.kernel.org/stable/c/18a08b5632809faa671279b3cd27d5f96cc5a3f0, https://git.kernel.org/stable/c/7a40b52d4442178bee0cf1c36bc450ab951cef0f, https://git.kernel.org/stable/c/9c40a68b7f97fa487e6c7e67fcf4f846a1f96692	O-LIN-LINU-050525/405

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overrun-local: Overrunning array veml6075_it_ms of 5 4-byte elements at element index 7 (byte offset 31) using index int_index (which evaluates to 7) This is hardening against potentially broken hardware. Good to have but not necessary to backport. **CVE ID: CVE-2025-40114**		
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/erdma: Prevent use-after-free in erdma_accept_newconn() After the erdma_cep_put(new_cep) being called, new_cep will be freed, and the following dereference will cause a UAF problem. Fix this issue. **CVE ID: CVE-2025-22088**	https://git.kernel.org/stable/c/667a628ab67d359166799fad89b3c6909599558a, https://git.kernel.org/stable/c/78411a133312ce7d8a3239c76a8fd85bca1cc10f, https://git.kernel.org/stable/c/7aa6bb5276d9fec98deb05615a086eeb893854ad	O-LIN-LINU-050525/406
Out-of-bounds Write	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_tunnel: fix geneve_opt type confusion addition When handling multiple NFTA_TUNNEL_KEY_OPTS_GENEVE attributes, the parsing logic should place every geneve_opt structure one by one compactly. Hence, when deciding the next geneve_opt position, the pointer addition should be in units of char *.	https://git.kernel.org/stable/c/0a93a710d6df334b828ea064c6d39fda34f901dc, https://git.kernel.org/stable/c/1b755d8eb1ace3870789d48fbd94f386ad6e30be, https://git.kernel.org/stable/c/28d88ee1e1cc8ac2d79aeb112717b97c5c833d43	O-LIN-LINU-050525/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			However, the current implementation erroneously does type conversion before the addition, which will lead to heap out-of-bounds write. [6.989857] ========== ========== ========== === [6.990293] BUG: KASAN: slab-out-of-bounds in nft_tunnel_obj_init+0x977/0xa70 [6.990725] Write of size 124 at addr ffff888005f18974 by task poc/178 [6.991162] [6.991259] CPU: 0 PID: 178 Comm: poc-oob-write Not tainted 6.1.132 #1 [6.991655] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 [6.992281] Call Trace: [6.992423] <TASK> [6.992586] dump_stack_lvl+0x44/0x5c [6.992801] print_report+0x184/0x4be [6.993790] kasan_report+0xc5/0x100 [6.994252] kasan_check_range+0xf3/0x1a0 [6.994486] memcpy+0x38/0x60 [6.994692] nft_tunnel_obj_init+0x977/0xa70 [6.995677] nft_obj_init+0x10c/0x1b0 [6.995891]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nf_tables_newobj+0x585/0x950 [6.996922] nfnetlink_rcv_batch+0xdf9/0x1020 [6.998997] nfnetlink_rcv+0x1df/0x220 [6.999537] netlink_unicast+0x395/0x530 [7.000771] netlink_sendmsg+0x3d0/0x6d0 [7.001462] __sock_sendmsg+0x99/0xa0 [7.001707] ___sys_sendmsg+0x409/0x450 [7.002391] __sys_sendmsg+0xfd/0x170 [7.003145] __sys_sendmsg+0xea/0x170 [7.004359] do_syscall_64+0x5e/0x90 [7.005817] entry_SYSCALL_64_after_hwframe+0x6e/0xd8 [7.006127] RIP: 0033:0x7ec756d4e407 [7.006339] Code: 48 89 fa 4c 89 df e8 38 aa 00 00 8b 93 08 03 00 00 59 5e 48 83 f8 fc 74 1a 5b c3 0f 1f 84 00 00 00 00 00 48 8b 44 24 10 0f 05 <5b> c3 0f 1f 80 00 00 00 00 83 e2 39 83 faf [7.007364] RSP: 002b:00007ffed5d46760 EFLAGS: 00000202 ORIG_RAX: 000000000000002e [7.007827] RAX: ffffffffffffffda RBX: 00007ec756cc4740 RCX: 00007ec756d4e407 [7.008223] RDX: 0000000000000000 RSI: 00007ffed5d467f0 RDI: 0000000000000003 [7.008620] RBP: 00007ffed5d468a0 R08:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 R09: 0000000000000000 [7.009039] R10: 0000000000000000 R11: 0000000000000202 R12: 0000000000000000 [7.009429] R13: 00007ffed5d478b0 R14: 00007ec756ee5000 R15: 00005cbd4e655cb8 Fix this bug with correct pointer addition and conversion in parse and dump code. **CVE ID: CVE-2025-22056**		
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/vkms: Fix use after free and double free on init error If the driver initialization fails, the vkms_exit() function might access an uninitialized or freed default_config pointer and it might double free it. Fix both possible errors by initializing default_config only when the driver initialization succeeded. **CVE ID: CVE-2025-22097**	https://git.kernel.org/stable/c/1f68f1cf09d06061eb549726ff8339e064eddebd, https://git.kernel.org/stable/c/49a69f67f53518bdd9b7eeebf019a2da6cc0e954, https://git.kernel.org/stable/c/561fc0c5cf41f646f3e9e61784cbc0fc832fb936	O-LIN-LINU-050525/408
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/core: Fix use-after-free when rename device name Syzbot reported a slab-use-after-free with the following call trace:	https://git.kernel.org/stable/c/0d6460b9d2a3ee380940bdf47680751ef91cb88e, https://git.kernel.org/stable/c/1d6a9e7449e2a0c1e2934eee7880ba8bd1e464c	O-LIN-LINU-050525/409

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			========== ========== ========== === BUG: KASAN: slab-use-after-free in nla_put+0xd3/0x150 lib/nlattr.c:1099 Read of size 5 at addr ffff888140ea1c60 by task syz.0.988/10025 CPU: 0 UID: 0 PID: 10025 Comm: syz.0.988 Not tainted 6.14.0-rc4-syzkaller-00859-gf77f12010f67 #0 Hardware name: Google Compute Engine, BIOS Google 02/12/2025 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:408 [inline] print_report+0x16e/0x5b0 mm/kasan/report.c:521 kasan_report+0x143/0x180 mm/kasan/report.c:634 kasan_check_range+0x282/0x290 mm/kasan/generic.c:189 __asan_memcpy+0x29/0x70 mm/kasan/shadow.c:105 nla_put+0xd3/0x150 lib/nlattr.c:1099 nla_put_string include/net/netlink.h:1621 [inline] fill_nldev_handle+0x16e/0x200 drivers/infiniband/core/nl	d, https://git.kernel.org/stable/c/56ec8580be5174b2b9774066e60f1aad56d201db	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dev.c:265 rdma_nl_notify_event+0x561/0xef0 drivers/infiniband/core/nldev.c:2857 ib_device_notify_register+0x22/0x230 drivers/infiniband/core/device.c:1344 ib_register_device+0x1292/0x1460 drivers/infiniband/core/device.c:1460 rxe_register_device+0x233/0x350 drivers/infiniband/sw/rxe/rxe_verbs.c:1540 rxe_net_add+0x74/0xf0 drivers/infiniband/sw/rxe/rxe_net.c:550 rxe_newlink+0xde/0x1a0 drivers/infiniband/sw/rxe/rxe.c:212 nldev_newlink+0x5ea/0x680 drivers/infiniband/core/nldev.c:1795 rdma_nl_rcv_skb drivers/infiniband/core/netlink.c:239 [inline] rdma_nl_rcv+0x6dd/0x9e0 drivers/infiniband/core/netlink.c:259 netlink_unicast_kernel net/netlink/af_netlink.c:1313 [inline] netlink_unicast+0x7f6/0x990 net/netlink/af_netlink.c:1339 netlink_sendmsg+0x8de/0xcb0 net/netlink/af_netlink.c:1883 sock_sendmsg_nosec		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/socket.c:709 [inline] __sock_sendmsg+0x221/0x270 net/socket.c:724 ___sys_sendmsg+0x53a/0x860 net/socket.c:2564 ___sys_sendmsg net/socket.c:2618 [inline] __sys_sendmsg+0x269/0x350 net/socket.c:2650 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f42d1b8d169 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 ... RSP: 002b:00007f42d2960038 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f42d1da6320 RCX: 00007f42d1b8d169 RDX: 0000000000000000 RSI: 00004000000002c0 RDI: 000000000000000c RBP: 00007f42d1c0e2a0 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f42d1da6320 R15: 00007ffe399344a8 </TASK> Allocated by task 10025: kasan_save_stack mm/kasan/common.c:47 [inline]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0x98/0xb0 mm/kasan/common.c:394 kasan_kmalloc include/linux/kasan.h:260 [inline] __do_kmalloc_node mm/slub.c:4294 [inline] __kmalloc_node_track_caller_noprof+0x28b/0x4c0 mm/slub.c:4313 __kmemdup_nul mm/util.c:61 [inline] kstrdup+0x42/0x100 mm/util.c:81 kobject_set_name_vargs+0x61/0x120 lib/kobject.c:274 dev_set_name+0xd5/0x120 drivers/base/core.c:3468 assign_name drivers/infiniband/core/device.c:1202 [inline] ib_register_device+0x178/0x1460 drivers/infiniband/core/device.c:1384 rxe_register_device+0x233/0x350 drivers/infiniband/sw/rxe/rxe_verbs.c:1540 rxe_net_add+0x74/0xf0 drivers/infiniband/sw/rxe/rxe_net.c:550 rxe_newlink+0xde/0x1a0 drivers/infiniband/sw/rxe/rxe.c:212 nldev_newlink+0x5ea/0x680 drivers/infiniband/core/nldev.c:1795 rdma_nl_rcv_skb		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drivers/infiniband/core/netlink.c:239 [inline] rdma_nl_rcv+0x6dd/0x9e0 drivers/infiniband/core/netlink.c:259 netlink_unicast_kernel net/netlink/af_netlink.c:1313 [inline] netlink_unicast+0x7f6/0x990 net/netlink/af_netlink.c:1339 netlink_sendmsg+0x8de/0xcb0 net ---truncated--- **CVE ID: CVE-2025-22085**		
Out-of-bounds Read	16-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate zero num_subauth before sub_auth is accessed Access psid->sub_auth[psid->num_subauth - 1] without checking if num_subauth is non-zero leads to an out-of-bounds read. This patch adds a validation step to ensure num_subauth != 0 before sub_auth is accessed. **CVE ID: CVE-2025-22038**	https://git.kernel.org/stable/c/0e36a3e080d6d8bd7a34e089345d043da4ac8283, https://git.kernel.org/stable/c/3ac65de111c686c95316ade660f8ba7aea3cd3cc, https://git.kernel.org/stable/c/56de7778a48560278c334077ace7b9ac4bfb2fd1	O-LIN-LINU-050525/410
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: ext4: fix OOB read when checking dotdot dir Mounting a corrupted filesystem with directory which contains '.' dir entry with rec_len == block size results in out-of-	https://git.kernel.org/stable/c/52a5509ab19a5d3afe301165d9b5787bba34d842, https://git.kernel.org/stable/c/53bc45da8d8da92ec07877f5922b130562eb4b00,	O-LIN-LINU-050525/411

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds read (later on, when the corrupted directory is removed). ext4_empty_dir() assumes every ext4 directory contains at least '.' and '..' as directory entries in the first data block. It first loads the '.' dir entry, performs sanity checks by calling ext4_check_dir_entry() and then uses its rec_len member to compute the location of '..' dir entry (in ext4_next_entry). It assumes the '..' dir entry fits into the same data block. If the rec_len of '.' is precisely one block (4KB), it slips through the sanity checks (it is considered the last directory entry in the data block) and leaves "struct ext4_dir_entry_2 *de" point exactly past the memory slot allocated to the data block. The following call to ext4_check_dir_entry() on new value of de then dereferences this pointer which results in out-of-bounds mem access. Fix this by extending __ext4_check_dir_entry() to check for '.' dir entries that reach the end of data block. Make sure to ignore the phony dir entries for checksum (by checking name_len for non-zero). Note: This is reported by KASAN as use-after-free in case another	https://git.kernel.org/stable/c/89503e5eae64637d0fa2218912b54660effe7d93	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			structure was recently freed from the slot past the bound, but it is really an OOB read. This issue was found by syzkaller tool. Call Trace: [38.594108] BUG: KASAN: slab-use-after-free in __ext4_check_dir_entry+0x67e/0x710 [38.594649] Read of size 2 at addr ffff88802b41a004 by task syz-executor/5375 [38.595158] [38.595288] CPU: 0 UID: 0 PID: 5375 Comm: syz-executor Not tainted 6.14.0-rc7 #1 [38.595298] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [38.595304] Call Trace: [38.595308] <TASK> [38.595311] dump_stack_lvl+0xa7/0xd0 [38.595325] print_address_description.constprop.0+0x2c/0x3f0 [38.595339] ? __ext4_check_dir_entry+0x67e/0x710 [38.595349] print_report+0xaa/0x250 [38.595359] ? __ext4_check_dir_entry+0x67e/0x710 [38.595368] ? kasan_addr_to_slab+0x9/0x90 [38.595378] kasan_report+0xab/0xe0 [38.595389] ? __ext4_check_dir_entry+0x67e/0x710 [38.595400]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__ext4_check_dir_entry+0x67e/0x710 [38.595410] ext4_empty_dir+0x465/0x990 [38.595421] ? __pfx_ext4_empty_dir+0x10/0x10 [38.595432] ext4_rmdir.part.0+0x29a/0xd10 [38.595441] ? __dquot_initialize+0x2a7/0xbf0 [38.595455] ? __pfx_ext4_rmdir.part.0+0x10/0x10 [38.595464] ? __pfx___dquot_initialize+0x10/0x10 [38.595478] ? down_write+0xdb/0x140 [38.595487] ? __pfx_down_write+0x10/0x10 [38.595497] ext4_rmdir+0xee/0x140 [38.595506] vfs_rmdir+0x209/0x670 [38.595517] ? lookup_one_qstr_excl+0x3b/0x190 [38.595529] do_rmdir+0x363/0x3c0 [38.595537] ? __pfx_do_rmdir+0x10/0x10 [38.595544] ? strncpy_from_user+0x1ff/0x2e0 [38.595561] __x64_sys_unlinkat+0xf0/0x130 [38.595570] do_syscall_64+0x5b/0x180 [38.595583] entry_SYSCALL_64_after_hwframe+0x76/0x7e **CVE ID: CVE-2025-37785**		
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has	https://git.kernel.org/stable/c/	O-LIN-LINU-050525/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been resolved: jfs: fix slab-out-of-bounds read in ea_get() During the "size_check" label in ea_get(), the code checks if the extended attribute list (xattr) size matches ea_size. If not, it logs "ea_get: invalid extended attribute" and calls print_hex_dump(). Here, EALIST_SIZE(ea_buf->xattr) returns 4110417968, which exceeds INT_MAX (2,147,483,647). Then ea_size is clamped: int size = clamp_t(int, ea_size, 0, EALIST_SIZE(ea_buf->xattr)); Although clamp_t aims to bound ea_size between 0 and 4110417968, the upper limit is treated as an int, causing an overflow above 2^31 - 1. This leads "size" to wrap around and become negative (-184549328). The "size" is then passed to print_hex_dump() (called "len" in print_hex_dump()), it is passed as type size_t (an unsigned type), this is then stored inside a variable called "int remaining", which is then assigned to "int linelen" which is then passed to hex_dump_to_buffer(). In print_hex_dump() the for loop, iterates	0beddc2a3f9b9cf7d8887973041e36c2d0fa3652, https://git.kernel.org/stable/c/16d3d36436492aa248b2d8045e75585ebcc2f34d, https://git.kernel.org/stable/c/3d6fd5b9c6acbc005e53d0211c7381f566babec1	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			through 0 to len-1, where len is 18446744073525002176, calling hex_dump_to_buffer() on each iteration:
			
			for (i = 0; i < len; i += rowsize) {
			linelen = min(remaining, rowsize);
			remaining -= rowsize;
			
			hex_dump_to_buffer (ptr + i, linelen, rowsize, groupsize,
			
			linebuf, sizeof(linebuf), ascii);
			
			...
			}
			
			The expected stopping condition (i < len) is effectively broken since len is corrupted and very large. This eventually leads to the "ptr+i" being passed to hex_dump_to_buffer() to get closer
			to the end of the actual bounds of "ptr", eventually an out of bounds access is done in hex_dump_to_buffer() in the following
			for loop:
			
			for (j = 0; j < len; j++) {
			if (linebuflen < lx + 2)
			
			goto overflow2;
			ch = ptr[j];
			...
			}		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			To fix this we should validate "EALIST_SIZE(ea_buf->xattr)" before it is utilised. **CVE ID: CVE-2025-39735**		
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: objtool, nvmet: Fix out-of-bounds stack access in nvmet_ctrl_state_show() The csts_state_names[] array only has six sparse entries, but the iteration code in nvmet_ctrl_state_show() iterates seven, resulting in a potential out-of-bounds stack read. Fix that. Fixes the following warning with an UBSAN kernel: vmlinux.o: warning: objtool: .text.nvmet_ctrl_state_show: unexpected end of section **CVE ID: CVE-2025-39778**	https://git.kernel.org/stable/c/0cc0efc58d6c741b2868d4af24874d7fec28a575, https://git.kernel.org/stable/c/107a23185d990e3df6638d9a84c835f963fe30a6, https://git.kernel.org/stable/c/1adc93a525fdee8e2b311e6d5fd93eb69714ca05	O-LIN-LINU-050525/413
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Apr-2025	7	In the Linux kernel, the following vulnerability has been resolved: exfat: fix random stack corruption after get_block When get_block is called with a buffer_head allocated on the stack, such as do_mpage_readpage, stack corruption due to buffer_head UAF may occur in the following race condition situation.	https://git.kernel.org/stable/c/1bb7ff4204b6d4927e982cd256286c09ed4fd8ca, https://git.kernel.org/stable/c/49b0a6ab8e528a0c1c50e37cef9b9c7c121365f2, https://git.kernel.org/stable/c/f7447286363dc1e410bf30b87d75168f3519f9cc	O-LIN-LINU-050525/414

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<CPU 0> <CPU 1> mpage_read_folio <<bh on stack>> do_mpage_readpage exfat_get_block bh_read __bh_read get_bh(bh) submit_bh wait_on_buffer ... end_buffer_read_sync __end_buffer_read_notouch unlock_buffer <<keep going>> ... ... <<bh is not valid out of mpage_read_folio>> . . another_function <<variable A on stack>> put_bh(bh) atomic_dec(bh->b_count) * stack corruption here * This patch returns -EAGAIN if a folio does not have buffers when bh_read needs to be called. By doing this, the caller can fallback to functions like block_read_full_folio(), create a buffer_head in the folio, and then call get_block again. Let's do not call bh_read() with on-stack buffer_head. **CVE ID: CVE-2025-22036**		
NULL	16-Apr-2025	5.5	In the Linux kernel, the	https://git.kern	O-LIN-LINU-

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			following vulnerability has been resolved: PCI/bwctrl: Fix NULL pointer dereference on bus number exhaustion When BIOS neglects to assign bus numbers to PCI bridges, the kernel attempts to correct that during PCI device enumeration. If it runs out of bus numbers, no pci_bus is allocated and the "subordinate" pointer in the bridge's pci_dev remains NULL. The PCIe bandwidth controller erroneously does not check for a NULL subordinate pointer and dereferences it on probe. Bandwidth control of unusable devices below the bridge is of questionable utility, so simply error out instead. This mirrors what PCIe hotplug does since commit 62e4492c3063 ("PCI: Prevent NULL dereference during pciehp probe"). The PCI core emits a message with KERN_INFO severity if it has run out of bus numbers. PCIe hotplug emits an additional message with KERN_ERR severity to inform the user that hotplug functionality is disabled at the bridge. A similar message for bandwidth control does not seem merited, given that its only purpose so far is to expose an up-to-date link speed	el.org/stable/c/1181924af78e5299ddec6e457789c02dd5966559, https://git.kernel.org/stable/c/667f053b05f00a007738cd7ed6fa1901de19dc7e, https://git.kernel.org/stable/c/d93d309013e89631630a12b1770d27e4be78362a	050525/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in sysfs and throttle the link speed on certain laptops with limited Thermal Design Power. So error out silently. User-visible messages: pci 0000:16:02.0: bridge configuration invalid ([bus 00-00]), reconfiguring [...] pci_bus 0000:45: busn_res: [bus 45-74] end is updated to 74 pci 0000:16:02.0: devices behind bridge are unusable because [bus 45-74] cannot be assigned for them [...] pcieport 0000:16:02.0: pciehp: Hotplug bridge without secondary bus, ignoring [...] BUG: kernel NULL pointer dereference RIP: pcie_update_link_speed pcie_bwnotif_enable pcie_bwnotif_probe pcie_port_probe_service really_probe **CVE ID: CVE-2025-22031**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix null pointer dereference in alloc_preauth_hash() The Client send malformed smb2 negotiate request. ksmbd return error response. Subsequently, the client can send smb2 session setup even thought conn->preauth_info is not allocated.	https://git.kernel.org/stable/c/8f216b33a5e1b3489c073b1ea1b3d7cb63c8dc4d, https://git.kernel.org/stable/c/b8eb243e670ecf30e91524dd12f7260dac07d335, https://git.kernel.org/stable/c/c8b5b7c5da7d0c31c9b7190b4a	O-LIN-LINU-050525/416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This patch add KSMBD_SESS_NEED_SETUP status of connection to ignore session setup request if smb2 negotiate phase is not complete. **CVE ID: CVE-2025-22037**	7bba5281fc4780	
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: staging: gpib: Fix Oops after disconnect in agilent usb If the agilent usb dongle is disconnected subsequent calls to the driver cause a NULL dereference Oops as the bus_interface is set to NULL on disconnect. This problem was introduced by setting usb_dev from the bus_interface for dev_xxx messages. Previously bus_interface was checked for NULL only in the functions directly calling usb_fill_bulk_urb or usb_control_msg. Check for valid bus_interface on all interface entry points and return -ENODEV if it is NULL. **CVE ID: CVE-2025-22051**	https://git.kernel.org/stable/c/50ef6e45bec79da4c5a01fad4dc23466ba255099, https://git.kernel.org/stable/c/8491e73a5223acb0a4b4d78c3f8b96aa9c5e774d, https://git.kernel.org/stable/c/e88633705078f40391a9afc6cc8ea3025e6f692b	O-LIN-LINU-050525/417
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: staging: gpib: Fix Oops after disconnect in ni_usb	https://git.kernel.org/stable/c/5dc98ba6f7304c188b267ef481281849638447bf,	O-LIN-LINU-050525/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If the usb dongle is disconnected subsequent calls to the driver cause a NULL dereference Oops as the bus_interface is set to NULL on disconnect. This problem was introduced by setting usb_dev from the bus_interface for dev_xxx messages. Previously bus_interface was checked for NULL only in the the functions directly calling usb_fill_bulk_urb or usb_control_msg. Check for valid bus_interface on all interface entry points and return -ENODEV if it is NULL. **CVE ID: CVE-2025-22052**	https://git.kernel.org/stable/c/a239c6e91b665f1837cf57b97fe638ef1baf2e78, https://git.kernel.org/stable/c/b2d8d7959077c5d4b11d0dc6bd2167791fd1c72e	
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: arm64: Don't call NULL in do_compat_alignment_fixup() do_alignment_t32_to_handler() only fixes up alignment faults for specific instructions; it returns NULL otherwise (e.g. LDREX). When that's the case, signal to the caller that it needs to proceed with the regular alignment fault handling (i.e. SIGBUS). Without this patch, the kernel panics:	https://git.kernel.org/stable/c/2df8ee605eb6806cd41c2095306db05206633a08, https://git.kernel.org/stable/c/617a4b0084a547917669fef2b54253cc9c064990, https://git.kernel.org/stable/c/c28f31deeacda307acfee2f18c0ad904e5123aac	O-LIN-LINU-050525/419

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000086000006 EC = 0x21: IABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x06: level 2 translation fault user pgtable: 4k pages, 48-bit VAs, pgdp=00000800164aa000 [0000000000000000] pgd=0800081fdbd22003, p4d=0800081fdbd22003, pud=08000815d51c6003, pmd=0000000000000000 Internal error: Oops: 0000000086000006 [#1] SMP Modules linked in: cfg80211 rfkill xt_nat xt_tcpudp xt_conntrack nft_chain_nat xt_MASQUERADE nf_nat nf_conntrack_netlink nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 xfrm_user xfrm_algo xt_addrtype nft_compat br_netfilter veth nvme_fa> libcrc32c crc32c_generic raid0 multipath linear dm_mod dax raid1 md_mod xhci_pci nvme xhci_hcd nvme_core t10_pi usbcore igb crc64_rocksoft crc64 crc_t10dif crct10dif_generic crct10dif_ce crct10dif_common usb_common i2c_algo_bit i2c> CPU: 2 PID: 3932954 Comm: WPEWebProcess Not tainted 6.1.0-31-arm64 #1 Debian 6.1.128-1 Hardware name:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GIGABYTE MP32-AR1-00/MP32-AR1-00, BIOS F18v (SCP: 1.08.20211002) 12/01/2021 pstate: 80400009 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : 0x0 lr : do_compat_alignment_fixup +0xd8/0x3dc sp : ffff80000f973dd0 x29: ffff80000f973dd0 x28: ffff081b42526180 x27: 0000000000000000 x26: 0000000000000000 x25: 0000000000000000 x24: 0000000000000000 x23: 0000000000000004 x22: 0000000000000000 x21: 0000000000000001 x20: 00000000e8551f00 x19: ffff80000f973eb0 x18: 0000000000000000 x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : ffffaebc949bc488 x8 : 0000000000000000 x7 : 0000000000000000 x6 : 0000000000000000 x5 : 0000000000400000 x4 : 0000ffffffffffe x3 : 0000000000000000 x2 : ffff80000f973eb0 x1 : 00000000e8551f00 x0 : 0000000000000001 Call trace: 0x0 do_alignment_fault+0x40/0x50 do_mem_abort+0x4c/0xa0 el0_da+0x48/0xf0 el0t_32_sync_handler+0x11		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0/0x140 el0t_32_sync+0x190/0x194 Code: bad PC value ---[end trace 0000000000000000]--- **CVE ID: CVE-2025-22033**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7921: fix kernel panic due to null pointer dereference Address a kernel panic caused by a null pointer dereference in the `mt792x_rx_get_wcid` function. The issue arises because the `deflink` structure is not properly initialized with the `sta` context. This patch ensures that the `deflink` structure is correctly linked to the `sta` context, preventing the null pointer dereference. BUG: kernel NULL pointer dereference, address: 0000000000000400 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 0 UID: 0 PID: 470 Comm: mt76-usb-rx phy Not tainted 6.12.13-gentoo-dist #1 Hardware name: /AMD HUDSON-M1, BIOS 4.6.4 11/15/2011 RIP: 0010:mt792x_rx_get_wcid+0x48/0x140 [mt792x_lib]	https://git.kernel.org/stable/c/0cfea60966e4b1239d20bebf02258295e189e82a, https://git.kernel.org/stable/c/5a57f8eb2a17d469d65cd1186cea26b798221d4a, https://git.kernel.org/stable/c/adc3fd2a2277b7cc0b61692463771bf9bd298036	O-LIN-LINU-050525/420

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RSP: 0018:ffffa147c055fd98 EFLAGS: 00010202 RAX: 0000000000000000 RBX: ffff8e9ecb652000 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000001 RDI: ffff8e9ecb652000 RBP: 0000000000000685 R08: ffff8e9ec6570000 R09: 0000000000000000 R10: ffff8e9ecd2ca000 R11: ffff8e9f22a217c0 R12: 0000000038010119 R13: 0000000080843801 R14: ffff8e9ec6570000 R15: ffff8e9ecb652000 FS: 0000000000000000(0000) GS:ffff8e9f22a00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000400 CR3: 000000000d2ea000 CR4: 00000000000006f0 Call Trace: <TASK> ? __die_body.cold+0x19/0x27 ? page_fault_oops+0x15a/0x2f0 ? search_module_extables+0x19/0x60 ? search_bpf_extables+0x5f/0x80 ? exc_page_fault+0x7e/0x180 ? asm_exc_page_fault+0x26/0x30 ? mt792x_rx_get_wcid+0x48/0x140 [mt792x_lib] mt7921_queue_rx_skb+0x1c6/0xaa0 [mt7921_common]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mt76u_alloc_queues+0x784/0x810 [mt76_usb] ? __pfx__mt76_worker_fn+0x10/0x10 [mt76] __mt76_worker_fn+0x4f/0x80 [mt76] kthread+0xd2/0x100 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x34/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> ---[end trace 0000000000000000]--- **CVE ID: CVE-2025-22032**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: arcnet: Add NULL check in com20020pci_probe() devm_kasprintf() returns NULL when memory allocation fails. Currently, com20020pci_probe() does not check for this case, which results in a NULL pointer dereference. Add NULL check after devm_kasprintf() to prevent this issue and ensure no resources are left allocated. **CVE ID: CVE-2025-22054**	https://git.kernel.org/stable/c/661cf5d102949898c931e81fd4e1c773afcdeafa, https://git.kernel.org/stable/c/8872261635044494ea7e58033a97c2d2ab12e05d4, https://git.kernel.org/stable/c/905a34dc1ad9a53a8aaaf8a759ea5dbaaa30418d	O-LIN-LINU-050525/421
NULL Pointer Dereference	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: remoteproc: core: Clear table_sz when	https://git.kernel.org/stable/c/068f6648ff5b0c7adeb6c363fae7fb188aa178fa, https://git.kern	O-LIN-LINU-050525/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rproc_shutdown There is case as below could trigger kernel dump: Use U-Boot to start remote processor(rproc) with resource table published to a fixed address by rproc. After Kernel boots up, stop the rproc, load a new firmware which doesn't have resource table ,and start rproc. When starting rproc with a firmware not have resource table, `memcpy(loaded_table, rproc->cached_table, rproc->table_sz)` will trigger dump, because rproc->cache_table is set to NULL during the last stop operation, but rproc->table_sz is still valid. This issue is found on i.MX8MP and i.MX9. Dump as below: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000096000004 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 user pgtable: 4k pages, 48-	el.org/stable/c/2df19f5f6f72da6f6ebab7cdb3a3b9f7686bb476, https://git.kernel.org/stable/c/6e66bca8cd51ebedd5d32426906a38e4a3c69c5f	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bit VAs, pgdp=000000010af63000 [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP Modules linked in: CPU: 2 UID: 0 PID: 1060 Comm: sh Not tainted 6.14.0-rc7-next-20250317-dirty #38 Hardware name: NXP i.MX8MPlus EVK board (DT) pstate: a0000005 (NzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __pi_memcpy_generic+0x110/0x22c lr : rproc_start+0x88/0x1e0 Call trace: __pi_memcpy_generic+0x110/0x22c (P) rproc_boot+0x198/0x57c state_store+0x40/0x104 dev_attr_store+0x18/0x2c sysfs_kf_write+0x7c/0x94 kernfs_fop_write_iter+0x120/0x1cc vfs_write+0x240/0x378 ksys_write+0x70/0x108 __arm64_sys_write+0x1c/0x28 invoke_syscall+0x48/0x10c el0_svc_common.constprop.0+0xc0/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x30/0xcc el0t_64_sync_handler+0x10c/0x138 el0t_64_sync+0x198/0x19c Clear rproc->table_sz to address the issue.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-38152		
Improper Validation of Array Index	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: clk: samsung: Fix UBSAN panic in samsung_clk_init() With UBSAN_ARRAY_BOUNDS=y, I'm hitting the below panic due to dereferencing `ctx->clk_data.hws` before setting `ctx->clk_data.num = nr_clks`. Move that up to fix the crash. UBSAN: array index out of bounds: 00000000f2005512 [#1] PREEMPT SMP <snip> Call trace: samsung_clk_init+0x110/0x124 (P) samsung_clk_init+0x48/0x124 (L) samsung_cmu_register_one+0x3c/0xa0 exynos_arm64_register_cmu+0x54/0x64 __gs101_cmu_top_of_clk_init_declare+0x28/0x60 ... **CVE ID: CVE-2025-39728**	https://git.kernel.org/stable/c/00307934eb94aaa0a99addfb37b9fe206f945004, https://git.kernel.org/stable/c/0fef48f4a70e45a93e73c39023c3a6ea624714d6, https://git.kernel.org/stable/c/157de9e48007a20c65d02fc0229a16f38134a72d	O-LIN-LINU-050525/423
NULL Pointer Dereference	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: staging: gpib: Fix cb7210 pcmcia Oops	https://git.kernel.org/stable/c/7ec50077d7f6647cb6ba3a2a20a6c26f51259c7d, https://git.kern	O-LIN-LINU-050525/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The pcmcia_driver struct was still only using the old .name initialization in the drv field. This led to a NULL pointer deref Oops in strcmp called from pcmcia_register_driver. Initialize the pcmcia_driver struct name field. **CVE ID: CVE-2025-39755**	el.org/stable/c/c1baf6528bcfd6a86842093ff3f8ff8caf309c12, https://git.kernel.org/stable/c/c82ae06f49e70d1c14ee9c76c392345856d050c9	
Improper Locking	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: ALSA: timer: Don't take register_mutex with copy_from/to_user() The infamous mmap_lock taken in copy_from/to_user() can be often problematic when it's called inside another mutex, as they might lead to deadlocks. In the case of ALSA timer code, the bad pattern is with guard(mutex)(&register_mutex) that covers copy_from/to_user() -- which was mistakenly introduced at converting to guard(), and it had been carefully worked around in the past. This patch fixes those pieces simply by moving copy_from/to_user() out of the register mutex lock again. **CVE ID: CVE-2025-23134**	https://git.kernel.org/stable/c/15291b561d8cc835a2eea76b394070cf8e072771, https://git.kernel.org/stable/c/296f7a9e15aab276db11206cbc1e2ae1215d7862, https://git.kernel.org/stable/c/3424c8f53bc63c87712a7fc22dc13d0cc85fb0d6	O-LIN-LINU-050525/425
NULL	16-Apr-2025	5.5	In the Linux kernel, the	https://git.kern	O-LIN-LINU-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			following vulnerability has been resolved: thermal: int340x: Add NULL check for adev Not all devices have an ACPI companion fwnode, so adev might be NULL. This is similar to the commit cd2fd6eab480 ("platform/x86: int3472: Check for adev == NULL"). Add a check for adev not being set and return -ENODEV in that case to avoid a possible NULL pointer deref in int3402_thermal_probe(). Note, under the same directory, int3400_thermal_probe() has such a check. [rjw: Subject edit, added Fixes:] **CVE ID: CVE-2025-23136**	el.org/stable/c/0c49f12c77b77a706fd41370c11910635e491845, https://git.kernel.org/stable/c/2542a3f70e563a9e70e7ded314286535a3321bdb, https://git.kernel.org/stable/c/3155d5261b518776d1b807d9d922669991bbee56	050525/426
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netlabel: Fix NULL pointer exception caused by CALIPSO on IPv4 sockets When calling netlbl_conn_setattr(), addr->sa_family is used to determine the function behavior. If sk is an IPv4 socket, but the connect function is called with an IPv6 address, the function calipso_sock_setattr() is triggered. Inside this function, the	https://git.kernel.org/stable/c/078aabd567de3d63d37d7673f714e309d369e6e2, https://git.kernel.org/stable/c/172a8a996a337206970467e871dd995ac07640b1, https://git.kernel.org/stable/c/1927d0bcd5b81e80971bf6b8eba267508bd1c78b	O-LIN-LINU-050525/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			following code is executed: sk_fullsock(__sk) ? inet_sk(__sk)->pinet6 : NULL; Since sk is an IPv4 socket, pinet6 is NULL, leading to a null pointer dereference. This patch fixes the issue by checking if inet6_sk(sk) returns a NULL pointer before accessing pinet6. **CVE ID: CVE-2025-22063**		
Off-by-one Error	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: LoongArch: BPF: Fix off-by-one error in build_prologue() Vincent reported that running BPF progs with tailcalls on LoongArch causes kernel hard lockup. Debugging the issues shows that the JITed image missing a jirl instruction at the end of the epilogue. There are two passes in JIT compiling, the first pass set the flags and the second pass generates JIT code based on those flags. With BPF progs mixing bpf2bpf and tailcalls, build_prologue() generates N insns in the first pass and then generates N+1 insns in the second pass. This makes epilogue_offset off by one and we will jump to some unexpected insn and cause lockup. Fix this by inserting a nop insn.	https://git.kernel.org/stable/c/205a2182c51ffebaef54d643e3745e720cded08b, https://git.kernel.org/stable/c/48b904de2408af5f936f0e03f48dfcddeab58aa0, https://git.kernel.org/stable/c/7e2586991e36663c9bc48c828b83eab180ad30a9	O-LIN-LINU-050525/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-37893		
NULL Pointer Dereference	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: x86/resctrl: Fix allocation of cleanest CLOSID on platforms with no monitors Commit 6eac36bb9eb0 ("x86/resctrl: Allocate the cleanest CLOSID by searching closid_num_dirty_rmid") added logic that causes resctrl to search for the CLOSID with the fewest dirty cache lines when creating a new control group, if requested by the arch code. This depends on the values read from the llc_occupancy counters. The logic is applicable to architectures where the CLOSID effectively forms part of the monitoring identifier and so do not allow complete freedom to choose an unused monitoring identifier for a given CLOSID. This support missed that some platforms may not have these counters. This causes a NULL pointer dereference when creating a new control group as the array was not allocated by dom_data_init(). As this feature isn't necessary on platforms that don't have cache occupancy monitors, add this to the	https://git.kernel.org/stable/c/93a418fc61da13d1ee4047d4d1327990f7a2816a, https://git.kernel.org/stable/c/a121798ae669351ec0697c94f71c3a692b2a755b, https://git.kernel.org/stable/c/a8a1bcc27d4607227088d80483164289b5348293	O-LIN-LINU-050525/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check that occurs when a new control group is allocated. **CVE ID: CVE-2025-38049**		
Affected Version(s): From (including) 6.14 Up to (excluding) 6.14.3					
Use After Free	18-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: HSI: ssi_protocol: Fix use after free vulnerability in ssi_protocol Driver Due to Race Condition In the ssi_protocol_probe() function, &ssi->work is bound with ssip_xmit_work(), In ssip_pn_setup(), the ssip_pn_xmit() function within the ssip_pn_ops structure is capable of starting the work. If we remove the module which will call ssi_protocol_remove() to make a cleanup, it will free ssi through kfree(ssi), while the work mentioned above will be used. The sequence of operations that may lead to a UAF bug is as follows: CPU0 CPU1 | ssip_xmit_work ssi_protocol_remove | kfree(ssi); | | struct hsi_client *cl = ssi->cl; | // use ssi Fix it by ensuring that the work is canceled before proceeding	https://git.kernel.org/stable/c/4b4194c9a7a8f92db39e8e86c85f4fb12ebbec4f, https://git.kernel.org/stable/c/58eb29dba712ab0f13af59ca2fe545f5ce360e78, https://git.kernel.org/stable/c/834e602d0cc7c743bfce734fad4a46cefc0f9ab1	O-LIN-LINU-050525/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the cleanup in ssi_protocol_remove(). **CVE ID: CVE-2025-37838**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.87					
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in ksmbd_sessions_deregister() In multichannel mode, UAF issue can occur in session_deregister when the second channel sets up a session through the connection of the first channel. session that is freed through the global session table can be accessed again through ->sessions of connection. **CVE ID: CVE-2025-22041**	https://git.kernel.org/stable/c/15a9605f8d69dc85005b1a00c31a050b8625e1aa, https://git.kernel.org/stable/c/33cc29e221df7a3085ae413e8c26c4e81a151153, https://git.kernel.org/stable/c/8ed0e9d2f410f63525afb8351181eea36c80bcf1	O-LIN-LINU-050525/431
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix session use-after-free in multichannel connection There is a race condition between session setup and ksmbd_sessions_deregister. The session can be freed before the connection is added to channel list of session. This patch check reference count of session before freeing it. **CVE ID: CVE-2025-22040**	https://git.kernel.org/stable/c/3980770cb1470054e6400fd9766866597572673 7, https://git.kernel.org/stable/c/596407adb9af1ee75fe7c7529607783d31b66e7f, https://git.kernel.org/stable/c/7dfbd4c43eed91dd2548a95236908025707a8dfd	O-LIN-LINU-050525/432
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/667a628ab67d359166799fad89	O-LIN-LINU-050525/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RDMA/erdma: Prevent use-after-free in erdma_accept_newconn() After the erdma_cep_put(new_cep) being called, new_cep will be freed, and the following dereference will cause a UAF problem. Fix this issue. **CVE ID: CVE-2025-22088**	b3c6909599558a, https://git.kernel.org/stable/c/78411a133312ce7d8a3239c76a8fd85bca1cc10f, https://git.kernel.org/stable/c/7aa6bb5276d9fec98deb05615a086eeb893854ad	
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/vkms: Fix use after free and double free on init error If the driver initialization fails, the vkms_exit() function might access an uninitialized or freed default_config pointer and it might double free it. Fix both possible errors by initializing default_config only when the driver initialization succeeded. **CVE ID: CVE-2025-22097**	https://git.kernel.org/stable/c/1f68f1cf09d06061eb549726ff8339e064eddebd, https://git.kernel.org/stable/c/49a69f67f53518bdd9b7eeebf019a2da6cc0e954, https://git.kernel.org/stable/c/561fc0c5cf41f646f3e9e61784cbc0fc832fb936	O-LIN-LINU-050525/434
Out-of-bounds Write	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_tunnel: fix geneve_opt type confusion addition When handling multiple NFTA_TUNNEL_KEY_OPTS_GENEVE attributes, the parsing logic should place every geneve_opt structure one by one compactly. Hence, when	https://git.kernel.org/stable/c/0a93a710d6df334b828ea064c6d39fda34f901dc, https://git.kernel.org/stable/c/1b755d8eb1ace3870789d48fbd94f386ad6e30be, https://git.kernel.org/stable/c/28d88ee1e1cc8	O-LIN-LINU-050525/435

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deciding the next geneve_opt position, the pointer addition should be in units of char *. However, the current implementation erroneously does type conversion before the addition, which will lead to heap out-of-bounds write. [6.989857] ========== ========== ========== === [6.990293] BUG: KASAN: slab-out-of-bounds in nft_tunnel_obj_init+0x977/0xa70 [6.990725] Write of size 124 at addr ffff888005f18974 by task poc/178 [6.991162] [6.991259] CPU: 0 PID: 178 Comm: poc-oob-write Not tainted 6.1.132 #1 [6.991655] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 [6.992281] Call Trace: [6.992423] <TASK> [6.992586] dump_stack_lvl+0x44/0x5c [6.992801] print_report+0x184/0x4be [6.993790] kasan_report+0xc5/0x100 [6.994252] kasan_check_range+0xf3/0x1a0 [6.994486] memcpy+0x38/0x60 [6.994692] nft_tunnel_obj_init+0x977/	ac2d79aeb112717b97c5c833d43	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0xa70 [6.995677] nft_obj_init+0x10c/0x1b0 [6.995891] nf_tables_newobj+0x585/0x950 [6.996922] nfnetlink_rcv_batch+0xdf9/0x1020 [6.998997] nfnetlink_rcv+0x1df/0x220 [6.999537] netlink_unicast+0x395/0x530 [7.000771] netlink_sendmsg+0x3d0/0x6d0 [7.001462] __sock_sendmsg+0x99/0xa0 [7.001707] ___sys_sendmsg+0x409/0x450 [7.002391] __sys_sendmsg+0xfd/0x170 [7.003145] __sys_sendmsg+0xea/0x170 [7.004359] do_syscall_64+0x5e/0x90 [7.005817] entry_SYSCALL_64_after_hwframe+0x6e/0xd8 [7.006127] RIP: 0033:0x7ec756d4e407 [7.006339] Code: 48 89 fa 4c 89 df e8 38 aa 00 00 8b 93 08 03 00 00 59 5e 48 83 f8 fc 74 1a 5b c3 0f 1f 84 00 00 00 00 00 48 8b 44 24 10 0f 05 <5b> c3 0f 1f 80 00 00 00 00 83 e2 39 83 faf [7.007364] RSP: 002b:00007ffed5d46760 EFLAGS: 00000202 ORIG_RAX: 000000000000002e [7.007827] RAX: ffffffffffffffda RBX: 00007ec756cc4740 RCX: 00007ec756d4e407 [7.008223] RDX: 0000000000000000 RSI:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			00007ffed5d467f0 RDI: 0000000000000003 [7.008620] RBP: 00007ffed5d468a0 R08: 0000000000000000 R09: 0000000000000000 [7.009039] R10: 0000000000000000 R11: 0000000000000202 R12: 0000000000000000 [7.009429] R13: 00007ffed5d478b0 R14: 00007ec756ee5000 R15: 00005cbd4e655cb8 Fix this bug with correct pointer addition and conversion in parse and dump code. **CVE ID: CVE-2025-22056**		
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: ext4: fix OOB read when checking dotdot dir Mounting a corrupted filesystem with directory which contains '.' dir entry with rec_len == block size results in out-of-bounds read (later on, when the corrupted directory is removed). ext4_empty_dir() assumes every ext4 directory contains at least '.' and '..' as directory entries in the first data block. It first loads the '.' dir entry, performs sanity checks by calling ext4_check_dir_entry() and then uses its rec_len member to compute the location of '..' dir entry (in ext4_next_entry). It assumes the '..' dir entry	https://git.kernel.org/stable/c/52a5509ab19a5d3afe301165d9b5787bba34d842, https://git.kernel.org/stable/c/53bc45da8d8da92ec07877f5922b130562eb4b00, https://git.kernel.org/stable/c/89503e5eae64637d0fa2218912b54660effe7d93	O-LIN-LINU-050525/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fits into the same data block. If the rec_len of '.' is precisely one block (4KB), it slips through the sanity checks (it is considered the last directory entry in the data block) and leaves "struct ext4_dir_entry_2 *de" point exactly past the memory slot allocated to the data block. The following call to ext4_check_dir_entry() on new value of de then dereferences this pointer which results in out-of-bounds mem access. Fix this by extending __ext4_check_dir_entry() to check for '.' dir entries that reach the end of data block. Make sure to ignore the phony dir entries for checksum (by checking name_len for non-zero). Note: This is reported by KASAN as use-after-free in case another structure was recently freed from the slot past the bound, but it is really an OOB read. This issue was found by syzkaller tool. Call Trace: [38.594108] BUG: KASAN: slab-use-after-free in __ext4_check_dir_entry+0x67e/0x710 [38.594649] Read of size 2 at addr ffff88802b41a004 by task syz-executor/5375 [38.595158] [38.595288] CPU: 0 UID: 0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PID: 5375 Comm: syz-executor Not tainted 6.14.0-rc7 #1 [38.595298] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [38.595304] Call Trace: [38.595308] <TASK> [38.595311] dump_stack_lvl+0xa7/0xd0 [38.595325] print_address_description.constprop.0+0x2c/0x3f0 [38.595339] ? __ext4_check_dir_entry+0x67e/0x710 [38.595349] print_report+0xaa/0x250 [38.595359] ? __ext4_check_dir_entry+0x67e/0x710 [38.595368] ? kasan_addr_to_slab+0x9/0x90 [38.595378] kasan_report+0xab/0xe0 [38.595389] ? __ext4_check_dir_entry+0x67e/0x710 [38.595400] __ext4_check_dir_entry+0x67e/0x710 [38.595410] ext4_empty_dir+0x465/0x990 [38.595421] ? __pfx_ext4_empty_dir+0x10/0x10 [38.595432] ext4_rmdir.part.0+0x29a/0xd10 [38.595441] ? __dquot_initialize+0x2a7/0xbf0 [38.595455] ? __pfx_ext4_rmdir.part.0+0x10/0x10 [38.595464] ?		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__pfx___dquot_initialize+0x10/0x10 [38.595478] ? down_write+0xdb/0x140 [38.595487] ? __pfx_down_write+0x10/0x10 [38.595497] ext4_rmdir+0xee/0x140 [38.595506] vfs_rmdir+0x209/0x670 [38.595517] ? lookup_one_qstr_excl+0x3b/0x190 [38.595529] do_rmdir+0x363/0x3c0 [38.595537] ? __pfx_do_rmdir+0x10/0x10 [38.595544] ? strncpy_from_user+0x1ff/0x2e0 [38.595561] __x64_sys_unlinkat+0xf0/0x130 [38.595570] do_syscall_64+0x5b/0x180 [38.595583] entry_SYSCALL_64_after_hwframe+0x76/0x7e **CVE ID: CVE-2025-37785**		
Out-of-bounds Read	16-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate zero num_subauth before sub_auth is accessed Access psid->sub_auth[psid->num_subauth - 1] without checking if num_subauth is non-zero leads to an out-of-bounds read. This patch adds a validation step to ensure num_subauth != 0 before sub_auth is accessed. **CVE ID: CVE-2025-22038**	https://git.kernel.org/stable/c/0e36a3e080d6d8bd7a34e089345d043da4ac8283, https://git.kernel.org/stable/c/3ac65de111c686c95316ade660f8ba7aea3cd3cc, https://git.kernel.org/stable/c/56de7778a48560278c334077ace7b9ac4bfb2fd1	O-LIN-LINU-050525/437

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: arm64: Don't call NULL in do_compat_alignment_fixup () do_alignment_t32_to_handler() only fixes up alignment faults for specific instructions; it returns NULL otherwise (e.g. LDREX). When that's the case, signal to the caller that it needs to proceed with the regular alignment fault handling (i.e. SIGBUS). Without this patch, the kernel panics: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000086000006 EC = 0x21: IABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x06: level 2 translation fault user pgtable: 4k pages, 48-bit VAs, pgdp=00000800164aa000 [0000000000000000] pgd=0800081fdbd22003, p4d=0800081fdbd22003, pud=08000815d51c6003, pmd=0000000000000000 Internal error: Oops: 0000000086000006 [#1] SMP Modules linked in: cfg80211 rfkill xt_nat xt_tcpudp xt_conntrack nft_chain_nat xt_MASQUERADE nf_nat nf_conntrack_netlink	https://git.kernel.org/stable/c/2df8ee605eb6806cd41c2095306db05206633a08, https://git.kernel.org/stable/c/617a4b0084a547917669fef2b54253cc9c064990, https://git.kernel.org/stable/c/c28f31deeacda307acfee2f18c0ad904e5123aac	O-LIN-LINU-050525/438

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 xfrm_user xfrm_algo xt_addrtype nft_compat br_netfilter veth nvme_fa> libcrc32c crc32c_generic raid0 multipath linear dm_mod dax raid1 md_mod xhci_pci nvme xhci_hcd nvme_core t10_pi usbcore igb crc64_rocksoft crc64 crc_t10dif crct10dif_generic crct10dif_ce crct10dif_common usb_common i2c_algo_bit i2c> CPU: 2 PID: 3932954 Comm: WPEWebProcess Not tainted 6.1.0-31-arm64 #1 Debian 6.1.128-1 Hardware name: GIGABYTE MP32-AR1-00/MP32-AR1-00, BIOS F18v (SCP: 1.08.20211002) 12/01/2021 pstate: 80400009 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : 0x0 lr : do_compat_alignment_fixup +0xd8/0x3dc sp : ffff80000f973dd0 x29: ffff80000f973dd0 x28: ffff081b42526180 x27: 0000000000000000 x26: 0000000000000000 x25: 0000000000000000 x24: 0000000000000000 x23: 0000000000000004 x22: 0000000000000000 x21: 0000000000000001 x20: 00000000e8551f00 x19: ffff80000f973eb0 x18: 0000000000000000 x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000000		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x10: 0000000000000000 x9 : ffffaebc949bc488 x8 : 0000000000000000 x7 : 0000000000000000 x6 : 0000000000000000 x5 : 0000000000400000 x4 : 0000ffffffffffffe x3 : 0000000000000000 x2 : ffff80000f973eb0 x1 : 00000000e8551f00 x0 : 0000000000000001 Call trace: 0x0 do_alignment_fault+0x40/0x50 do_mem_abort+0x4c/0xa0 el0_da+0x48/0xf0 el0t_32_sync_handler+0x110/0x140 el0t_32_sync+0x190/0x194 Code: bad PC value ---[end trace 0000000000000000]--- **CVE ID: CVE-2025-22033**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netlabel: Fix NULL pointer exception caused by CALIPSO on IPv4 sockets When calling netlbl_conn_setattr(), addr->sa_family is used to determine the function behavior. If sk is an IPv4 socket, but the connect function is called with an IPv6 address, the function calipso_sock_setattr() is triggered. Inside this function, the following code is executed:	https://git.kernel.org/stable/c/078aabd567de3d63d37d7673f714e309d369e6e2, https://git.kernel.org/stable/c/172a8a996a337206970467e871dd995ac07640b1, https://git.kernel.org/stable/c/1927d0bcd5b81e80971bf6b8eba267508bd1c78b	O-LIN-LINU-050525/439

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sk_fullsock(__sk) ? inet_sk(__sk)->pinet6 : NULL; Since sk is an IPv4 socket, pinet6 is NULL, leading to a null pointer dereference. This patch fixes the issue by checking if inet6_sk(sk) returns a NULL pointer before accessing pinet6. **CVE ID: CVE-2025-22063**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: thermal: int340x: Add NULL check for adev Not all devices have an ACPI companion fwnode, so adev might be NULL. This is similar to the commit cd2fd6eab480 ("platform/x86: int3472: Check for adev == NULL"). Add a check for adev not being set and return -ENODEV in that case to avoid a possible NULL pointer deref in int3402_thermal_probe(). Note, under the same directory, int3400_thermal_probe() has such a check. [rjw: Subject edit, added Fixes:] **CVE ID: CVE-2025-23136**	https://git.kernel.org/stable/c/0c49f12c77b77a706fd41370c11910635e491845, https://git.kernel.org/stable/c/2542a3f70e563a9e70e7ded314286535a3321bdb, https://git.kernel.org/stable/c/3155d5261b518776d1b807d9d922669991bbee56	O-LIN-LINU-050525/440
NULL Pointer Dereference	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: remoteproc: core: Clear	https://git.kernel.org/stable/c/068f6648ff5b0c7adeb6c363fae7fb188aa178fa,	O-LIN-LINU-050525/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			table_sz when rproc_shutdown There is case as below could trigger kernel dump: Use U-Boot to start remote processor(rproc) with resource table published to a fixed address by rproc. After Kernel boots up, stop the rproc, load a new firmware which doesn't have resource table ,and start rproc. When starting rproc with a firmware not have resource table, `memcpy(loaded_table, rproc->cached_table, rproc->table_sz)` will trigger dump, because rproc->cache_table is set to NULL during the last stop operation, but rproc->table_sz is still valid. This issue is found on i.MX8MP and i.MX9. Dump as below: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000096000004 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0	https://git.kernel.org/stable/c/2df19f5f6f72da6f6ebab7cdb3a3b9f7686bb476, https://git.kernel.org/stable/c/6e66bca8cd51ebedd5d32426906a38e4a3c69c5f	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user pgtable: 4k pages, 48-bit VAs, pgdp=000000010af63000 [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP Modules linked in: CPU: 2 UID: 0 PID: 1060 Comm: sh Not tainted 6.14.0-rc7-next-20250317-dirty #38 Hardware name: NXP i.MX8MPlus EVK board (DT) pstate: a0000005 (NzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __pi_memcpy_generic+0x110/0x22c lr : rproc_start+0x88/0x1e0 Call trace: __pi_memcpy_generic+0x110/0x22c (P) rproc_boot+0x198/0x57c state_store+0x40/0x104 dev_attr_store+0x18/0x2c sysfs_kf_write+0x7c/0x94 kernfs_fop_write_iter+0x120/0x1cc vfs_write+0x240/0x378 ksys_write+0x70/0x108 __arm64_sys_write+0x1c/0x28 invoke_syscall+0x48/0x10c el0_svc_common.constprop.0+0xc0/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x30/0xcc el0t_64_sync_handler+0x10c/0x138 el0t_64_sync+0x198/0x19c Clear rproc->table_sz to address the issue.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-38152		
Improper Validation of Array Index	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: clk: samsung: Fix UBSAN panic in samsung_clk_init() With UBSAN_ARRAY_BOUNDS=y, I'm hitting the below panic due to dereferencing `ctx->clk_data.hws` before setting `ctx->clk_data.num = nr_clks`. Move that up to fix the crash. UBSAN: array index out of bounds: 00000000f2005512 [#1] PREEMPT SMP <snip> Call trace: samsung_clk_init+0x110/0x124 (P) samsung_clk_init+0x48/0x124 (L) samsung_cmu_register_one+0x3c/0xa0 exynos_arm64_register_cmu+0x54/0x64 __gs101_cmu_top_of_clk_init_declare+0x28/0x60 ... **CVE ID: CVE-2025-39728**	https://git.kernel.org/stable/c/00307934eb94aaa0a99addfb37b9fe206f945004, https://git.kernel.org/stable/c/0fef48f4a70e45a93e73c39023c3a6ea624714d6, https://git.kernel.org/stable/c/157de9e48007a20c65d02fc0229a16f38134a72d	O-LIN-LINU-050525/442
Off-by-one Error	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: LoongArch: BPF: Fix off-by-one error in build_prologue()	https://git.kernel.org/stable/c/205a2182c51ffebaef54d643e3745e720cded08b, https://git.kernel.org/stable/c/	O-LIN-LINU-050525/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vincent reported that running BPF progs with tailcalls on LoongArch causes kernel hard lockup. Debugging the issues shows that the JITed image missing a jirl instruction at the end of the epilogue. There are two passes in JIT compiling, the first pass set the flags and the second pass generates JIT code based on those flags. With BPF progs mixing bpf2bpf and tailcalls, build_prologue() generates N insns in the first pass and then generates N+1 insns in the second pass. This makes epilogue_offset off by one and we will jump to some unexpected insn and cause lockup. Fix this by inserting a nop insn. **CVE ID: CVE-2025-37893**	48b904de2408af5f936f0e03f48dfcddeab58aa0, https://git.kernel.org/stable/c/7e2586991e36663c9bc48c828b83eab180ad30a9	
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.88					
Use After Free	18-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: HSI: ssi_protocol: Fix use after free vulnerability in ssi_protocol Driver Due to Race Condition In the ssi_protocol_probe() function, &ssi->work is bound with ssip_xmit_work(), In ssip_pn_setup(), the ssip_pn_xmit() function within the ssip_pn_ops structure is capable of starting the work.	https://git.kernel.org/stable/c/4b4194c9a7a8f92db39e8e86c85f4fb12ebbec4f, https://git.kernel.org/stable/c/58eb29dba712ab0f13af59ca2fe545f5ce360e78, https://git.kernel.org/stable/c/834e602d0cc7c743bfce734fad4a46cefc0f9ab1	O-LIN-LINU-050525/444

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If we remove the module which will call ssi_protocol_remove() to make a cleanup, it will free ssi through kfree(ssi), while the work mentioned above will be used. The sequence of operations that may lead to a UAF bug is as follows: CPU0 CPU1 | ssip_xmit_work ssi_protocol_remove | kfree(ssi); | | struct hsi_client *cl = ssi->cl; | // use ssi Fix it by ensuring that the work is canceled before proceeding with the cleanup in ssi_protocol_remove(). **CVE ID: CVE-2025-37838**		
Affected Version(s): From (including) 6.4.13 Up to (excluding) 6.6.87					
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix use-after-free in print_graph_function_flags during tracer switching Kairui reported a UAF issue in print_graph_function_flags() during ftrace stress testing [1]. This issue can be reproduced if puting a 'mdelay(10)' after 'mutex_unlock(&trace_types_lock)' in s_start(), and executing the following script:	https://git.kernel.org/stable/c/099ef3385800828b74933a96c117574637c3fb3a, https://git.kernel.org/stable/c/42561fe62c3628ea3bc9623f64f047605e98857f, https://git.kernel.org/stable/c/70be951bc01e4a0e10d443f3510bb17426f257fb	O-LIN-LINU-050525/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			$ echo function_graph > current_tracer
			$ cat trace > /dev/null &
			$ sleep 5 # Ensure the 'cat' reaches the 'mdelay(10)' point
			$ echo timerlat > current_tracer
			
			The root cause lies in the two calls to print_graph_function_flags within print_trace_line during each s_show():
			
			* One through 'iter->trace->print_line()';
			* Another through 'event->funcs->trace()', which is hidden in print_trace_fmt() before print_trace_line returns.
			
			Tracer switching only updates the former, while the latter continues to use the print_line function of the old tracer, which in the script above is print_graph_function_flags.
			
			Moreover, when switching from the 'function_graph' tracer to the 'timerlat' tracer, s_start only calls graph_trace_close of the 'function_graph' tracer to free 'iter->private', but does not set it to NULL. This provides an opportunity for 'event->funcs->trace()' to use an invalid 'iter->private'.
			
			To fix this issue, set 'iter->private' to NULL immediately after freeing it in graph_trace_close(),		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ensuring that an invalid pointer is not passed to other tracers. Additionally, clean up the unnecessary 'iter->private = NULL' during each 'cat trace' when using wakeup and irqsoff tracers. [1] https://lore.kernel.org/all/20231112150030.84609-1-ryncsn@gmail.com/ **CVE ID: CVE-2025-22035**		
Affected Version(s): From (including) 6.6.64 Up to (excluding) 6.6.87					
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: jfs: fix slab-out-of-bounds read in ea_get() During the "size_check" label in ea_get(), the code checks if the extended attribute list (xattr) size matches ea_size. If not, it logs "ea_get: invalid extended attribute" and calls print_hex_dump(). Here, EALIST_SIZE(ea_buf->xattr) returns 4110417968, which exceeds INT_MAX (2,147,483,647). Then ea_size is clamped: int size = clamp_t(int, ea_size, 0, EALIST_SIZE(ea_buf->xattr)); Although clamp_t aims to bound ea_size between 0 and 4110417968, the upper limit is treated as an int, causing an overflow above	https://git.kernel.org/stable/c/0beddc2a3f9b9cf7d8887973041e36c2d0fa3652, https://git.kernel.org/stable/c/16d3d36436492aa248b2d8045e75585ebcc2f34d, https://git.kernel.org/stable/c/3d6fd5b9c6acbc005e53d0211c7381f566babec1	O-LIN-LINU-050525/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			2^31 - 1. This leads "size" to wrap around and become negative (-184549328).
			
			The "size" is then passed to print_hex_dump() (called "len" in print_hex_dump()), it is passed as type size_t (an unsigned type), this is then stored inside a variable called "int remaining", which is then assigned to "int linelen" which is then passed to hex_dump_to_buffer(). In print_hex_dump() the for loop, iterates through 0 to len-1, where len is 18446744073525002176, calling hex_dump_to_buffer() on each iteration:
			
			for (i = 0; i < len; i += rowsize) {
			linelen = min(remaining, rowsize);
			remaining -= rowsize;
			
			hex_dump_to_buffer (ptr + i, linelen, rowsize, groupsize,
			
			linebuf, sizeof(linebuf), ascii);
			
			...
			}
			
			The expected stopping condition (i < len) is effectively broken since len is corrupted and very large. This eventually leads to the "ptr+i" being passed to		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			hex_dump_to_buffer() to get closer to the end of the actual bounds of "ptr", eventually an out of bounds access is done in hex_dump_to_buffer() in the following for loop:
			
			for (j = 0; j < len; j++) {
			if (linebuflen < lx + 2)
			
			goto overflow2;
			ch = ptr[j];
			...
			}
			
			To fix this we should validate "EALIST_SIZE(ea_buf->xattr)" before it is utilised.
			
			CVE ID: CVE-2025-39735		

Affected Version(s): From (including) 6.6.7 Up to (excluding) 6.6.87					
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: arcnet: Add NULL check in com20020pci_probe() devm_kasprintf() returns NULL when memory allocation fails. Currently, com20020pci_probe() does not check for this case, which results in a NULL pointer dereference. Add NULL check after devm_kasprintf() to prevent this issue and ensure no resources are left allocated. **CVE ID: CVE-2025-22054**	https://git.kernel.org/stable/c/661cf5d102949898c931e81fd4e1c773afcdeafa, https://git.kernel.org/stable/c/8872261635044 94ea7e58033a97c2d2ab12e05d4, https://git.kernel.org/stable/c/905a34dc1ad9a53a8aaaf8a759ea5dbaaa30418d	O-LIN-LINU-050525/447

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.13					
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in ksmbd_sessions_deregister() In multichannel mode, UAF issue can occur in session_deregister when the second channel sets up a session through the connection of the first channel. session that is freed through the global session table can be accessed again through ->sessions of connection. **CVE ID: CVE-2025-22041**	https://git.kernel.org/stable/c/15a9605f8d69dc85005b1a00c31a050b8625e1aa, https://git.kernel.org/stable/c/33cc29e221df7a3085ae413e8c26c4e81a151153, https://git.kernel.org/stable/c/8ed0e9d2f410f63525afb8351181eea36c80bcf1	O-LIN-LINU-050525/448
Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.23					
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix session use-after-free in multichannel connection There is a race condition between session setup and ksmbd_sessions_deregister. The session can be freed before the connection is added to channel list of session. This patch check reference count of session before freeing it. **CVE ID: CVE-2025-22040**	https://git.kernel.org/stable/c/3980770cb1470054e6400fd9766866597572673 7, https://git.kernel.org/stable/c/596407adb9af1ee75fe7c7529607783d31b66e7f, https://git.kernel.org/stable/c/7dfbd4c43eed91dd2548a95236908025707a8dfd	O-LIN-LINU-050525/449
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix use-after-free in print_graph_function_flags	https://git.kernel.org/stable/c/099ef3385800828b74933a96c117574637c3fb3a,	O-LIN-LINU-050525/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			during tracer switching
			
			Kairui reported a UAF issue in print_graph_function_flags() during ftrace stress testing [1]. This issue can be reproduced if puting a 'mdelay(10)' after 'mutex_unlock(&trace_types_lock)' in s_start(), and executing the following script:
			
			$ echo function_graph > current_tracer
			$ cat trace > /dev/null &
			$ sleep 5 # Ensure the 'cat' reaches the 'mdelay(10)' point
			$ echo timerlat > current_tracer
			
			The root cause lies in the two calls to print_graph_function_flags within print_trace_line during each s_show():
			
			* One through 'iter->trace->print_line()';
			* Another through 'event->funcs->trace()', which is hidden in print_trace_fmt() before print_trace_line returns.
			
			Tracer switching only updates the former, while the latter continues to use the print_line function of the old tracer, which in the script above is print_graph_function_flags.
			
			Moreover, when switching from the 'function_graph' tracer to the 'timerlat' tracer, s_start only calls graph_trace_close of
				https://git.kernel.org/stable/c/42561fe62c3628ea3bc9623f64f047605e98857f, https://git.kernel.org/stable/c/70be951bc01e4a0e10d443f3510bb17426f257fb	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the 'function_graph' tracer to free 'iter->private', but does not set it to NULL. This provides an opportunity for 'event->funcs->trace()' to use an invalid 'iter->private'. To fix this issue, set 'iter->private' to NULL immediately after freeing it in graph_trace_close(), ensuring that an invalid pointer is not passed to other tracers. Additionally, clean up the unnecessary 'iter->private = NULL' during each 'cat trace' when using wakeup and irqsoff tracers. [1] https://lore.kernel.org/all/20231112150030.84609-1-ryncsn@gmail.com/ **CVE ID: CVE-2025-22035**		
Out-of-bounds Write	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_tunnel: fix geneve_opt type confusion addition When handling multiple NFTA_TUNNEL_KEY_OPTS_GENEVE attributes, the parsing logic should place every geneve_opt structure one by one compactly. Hence, when deciding the next geneve_opt position, the pointer addition should be in units of char *.	https://git.kernel.org/stable/c/0a93a710d6df334b828ea064c6d39fda34f901dc, https://git.kernel.org/stable/c/1b755d8eb1ace3870789d48fbd94f386ad6e30be, https://git.kernel.org/stable/c/28d88ee1e1cc8ac2d79aeb112717b97c5c833d43	O-LIN-LINU-050525/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			However, the current implementation erroneously does type conversion before the addition, which will lead to heap out-of-bounds write. [6.989857] ========== ========== ========== === [6.990293] BUG: KASAN: slab-out-of-bounds in nft_tunnel_obj_init+0x977/0xa70 [6.990725] Write of size 124 at addr ffff888005f18974 by task poc/178 [6.991162] [6.991259] CPU: 0 PID: 178 Comm: poc-oob-write Not tainted 6.1.132 #1 [6.991655] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 [6.992281] Call Trace: [6.992423] <TASK> [6.992586] dump_stack_lvl+0x44/0x5c [6.992801] print_report+0x184/0x4be [6.993790] kasan_report+0xc5/0x100 [6.994252] kasan_check_range+0xf3/0x1a0 [6.994486] memcpy+0x38/0x60 [6.994692] nft_tunnel_obj_init+0x977/0xa70 [6.995677] nft_obj_init+0x10c/0x1b0 [6.995891] nf_tables_newobj+0x585/0x		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			950 [6.996922] nfnetlink_rcv_batch+0xdf9/0x1020 [6.998997] nfnetlink_rcv+0x1df/0x220 [6.999537] netlink_unicast+0x395/0x530 [7.000771] netlink_sendmsg+0x3d0/0x6d0 [7.001462] __sock_sendmsg+0x99/0xa0 [7.001707] ____sys_sendmsg+0x409/0x450 [7.002391] ___sys_sendmsg+0xfd/0x170 [7.003145] __sys_sendmsg+0xea/0x170 [7.004359] do_syscall_64+0x5e/0x90 [7.005817] entry_SYSCALL_64_after_hwframe+0x6e/0xd8 [7.006127] RIP: 0033:0x7ec756d4e407 [7.006339] Code: 48 89 fa 4c 89 df e8 38 aa 00 00 8b 93 08 03 00 00 59 5e 48 83 f8 fc 74 1a 5b c3 0f 1f 84 00 00 00 00 00 48 8b 44 24 10 0f 05 <5b> c3 0f 1f 80 00 00 00 00 83 e2 39 83 faf [7.007364] RSP: 002b:00007ffed5d46760 EFLAGS: 00000202 ORIG_RAX: 000000000000002e [7.007827] RAX: ffffffffffffffda RBX: 00007ec756cc4740 RCX: 00007ec756d4e407 [7.008223] RDX: 0000000000000000 RSI: 00007ffed5d467f0 RDI: 0000000000000003 [7.008620] RBP: 00007ffed5d468a0 R08: 0000000000000000 R09:		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 [7.009039] R10: 0000000000000000 R11: 0000000000000202 R12: 0000000000000000 [7.009429] R13: 00007ffed5d478b0 R14: 00007ec756ee5000 R15: 00005cbd4e655cb8 Fix this bug with correct pointer addition and conversion in parse and dump code. **CVE ID: CVE-2025-22056**		
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/vkms: Fix use after free and double free on init error If the driver initialization fails, the vkms_exit() function might access an uninitialized or freed default_config pointer and it might double free it. Fix both possible errors by initializing default_config only when the driver initialization succeeded. **CVE ID: CVE-2025-22097**	https://git.kernel.org/stable/c/1f68f1cf09d06061eb549726ff8339e064eddebd, https://git.kernel.org/stable/c/49a69f67f53518bdd9b7eeebf019a2da6cc0e954, https://git.kernel.org/stable/c/561fc0c5cf41f646f3e9e61784cbc0fc832fb936	O-LIN-LINU-050525/452
Use After Free	16-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: RDMA/erdma: Prevent use-after-free in erdma_accept_newconn() After the erdma_cep_put(new_cep) being called, new_cep will be freed,	https://git.kernel.org/stable/c/667a628ab67d359166799fad89b3c6909599558a, https://git.kernel.org/stable/c/78411a133312ce7d8a3239c76a8fd85bca1cc10f, https://git.kern	O-LIN-LINU-050525/453

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the following dereference will cause a UAF problem. Fix this issue. **CVE ID: CVE-2025-22088**	el.org/stable/c/7aa6bb5276d9fec98deb05615a086eeb893854ad	
Out-of-bounds Read	16-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate zero num_subauth before sub_auth is accessed Access psid->sub_auth[psid->num_subauth - 1] without checking if num_subauth is non-zero leads to an out-of-bounds read. This patch adds a validation step to ensure num_subauth != 0 before sub_auth is accessed. **CVE ID: CVE-2025-22038**	https://git.kernel.org/stable/c/0e36a3e080d6d8bd7a34e089345d043da4ac8283, https://git.kernel.org/stable/c/3ac65de111c686c95316ade660f8ba7aea3cd3cc, https://git.kernel.org/stable/c/56de7778a48560278c334077ace7b9ac4bfb2fd1	O-LIN-LINU-050525/454
Out-of-bounds Read	18-Apr-2025	7.1	In the Linux kernel, the following vulnerability has been resolved: ext4: fix OOB read when checking dotdot dir Mounting a corrupted filesystem with directory which contains '.' dir entry with rec_len == block size results in out-of-bounds read (later on, when the corrupted directory is removed). ext4_empty_dir() assumes every ext4 directory contains at least '.' and '..' as directory entries in the first data block. It first loads the '.' dir entry, performs sanity checks by calling ext4_check_dir_entry() and then uses its rec_len	https://git.kernel.org/stable/c/52a5509ab19a5d3afe301165d9b5787bba34d842, https://git.kernel.org/stable/c/53bc45da8d8da92ec07877f5922b130562eb4b00, https://git.kernel.org/stable/c/89503e5eae64637d0fa2218912b54660effe7d93	O-LIN-LINU-050525/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			member to compute the location of '..' dir entry (in ext4_next_entry). It assumes the '..' dir entry fits into the same data block. If the rec_len of '.' is precisely one block (4KB), it slips through the sanity checks (it is considered the last directory entry in the data block) and leaves "struct ext4_dir_entry_2 *de" point exactly past the memory slot allocated to the data block. The following call to ext4_check_dir_entry() on new value of de then dereferences this pointer which results in out-of-bounds mem access. Fix this by extending __ext4_check_dir_entry() to check for '.' dir entries that reach the end of data block. Make sure to ignore the phony dir entries for checksum (by checking name_len for non-zero). Note: This is reported by KASAN as use-after-free in case another structure was recently freed from the slot past the bound, but it is really an OOB read. This issue was found by syzkaller tool. Call Trace: [38.594108] BUG: KASAN: slab-use-after-free in __ext4_check_dir_entry+0x67e/0x710 [38.594649] Read of size 2		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			at addr ffff88802b41a004 by task syz-executor/5375 [38.595158] [38.595288] CPU: 0 UID: 0 PID: 5375 Comm: syz-executor Not tainted 6.14.0-rc7 #1 [38.595298] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 [38.595304] Call Trace: [38.595308] <TASK> [38.595311] dump_stack_lvl+0xa7/0xd0 [38.595325] print_address_description.constprop.0+0x2c/0x3f0 [38.595339] ? __ext4_check_dir_entry+0x67e/0x710 [38.595349] print_report+0xaa/0x250 [38.595359] ? __ext4_check_dir_entry+0x67e/0x710 [38.595368] ? kasan_addr_to_slab+0x9/0x90 [38.595378] kasan_report+0xab/0xe0 [38.595389] ? __ext4_check_dir_entry+0x67e/0x710 [38.595400] __ext4_check_dir_entry+0x67e/0x710 [38.595410] ext4_empty_dir+0x465/0x990 [38.595421] ? __pfx_ext4_empty_dir+0x10/0x10 [38.595432] ext4_rmdir.part.0+0x29a/0xd10 [38.595441] ? __dquot_initialize+0x2a7/0xbf0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[38.595455] ? __pfx_ext4_rmdir.part.0+0x10/0x10 [38.595464] ? __pfx___dquot_initialize+0x10/0x10 [38.595478] ? down_write+0xdb/0x140 [38.595487] ? __pfx_down_write+0x10/0x10 [38.595497] ext4_rmdir+0xee/0x140 [38.595506] vfs_rmdir+0x209/0x670 [38.595517] ? lookup_one_qstr_excl+0x3b/0x190 [38.595529] do_rmdir+0x363/0x3c0 [38.595537] ? __pfx_do_rmdir+0x10/0x10 [38.595544] ? strncpy_from_user+0x1ff/0x2e0 [38.595561] __x64_sys_unlinkat+0xf0/0x130 [38.595570] do_syscall_64+0x5b/0x180 [38.595583] entry_SYSCALL_64_after_hwframe+0x76/0x7e **CVE ID: CVE-2025-37785**		
Off-by-one Error	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: LoongArch: BPF: Fix off-by-one error in build_prologue() Vincent reported that running BPF progs with tailcalls on LoongArch causes kernel hard lockup. Debugging the issues shows that the JITed image missing a jirl instruction at the end of the	https://git.kernel.org/stable/c/205a2182c51ffebaef54d643e3745e720cded08b, https://git.kernel.org/stable/c/48b904de2408af5f936f0e03f48dfcddeab58aa0, https://git.kernel.org/stable/c/7e2586991e36663c9bc48c828b83eab180ad30a9	O-LIN-LINU-050525/456

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			epilogue. There are two passes in JIT compiling, the first pass set the flags and the second pass generates JIT code based on those flags. With BPF progs mixing bpf2bpf and tailcalls, build_prologue() generates N insns in the first pass and then generates N+1 insns in the second pass. This makes epilogue_offset off by one and we will jump to some unexpected insn and cause lockup. Fix this by inserting a nop insn. **CVE ID: CVE-2025-37893**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netlabel: Fix NULL pointer exception caused by CALIPSO on IPv4 sockets When calling netlbl_conn_setattr(), addr->sa_family is used to determine the function behavior. If sk is an IPv4 socket, but the connect function is called with an IPv6 address, the function calipso_sock_setattr() is triggered. Inside this function, the following code is executed: sk_fullsock(__sk) ? inet_sk(__sk)->pinet6 : NULL; Since sk is an IPv4 socket, pinet6 is NULL, leading to a null pointer dereference.	https://git.kernel.org/stable/c/078aabd567de3d63d37d7673f714e309d369e6e2, https://git.kernel.org/stable/c/172a8a996a337206970467e871dd995ac07640b1, https://git.kernel.org/stable/c/1927d0bcd5b81e80971bf6b8eba267508bd1c78b	O-LIN-LINU-050525/457

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This patch fixes the issue by checking if inet6_sk(sk) returns a NULL pointer before accessing pinet6. **CVE ID: CVE-2025-22063**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: thermal: int340x: Add NULL check for adev Not all devices have an ACPI companion fwnode, so adev might be NULL. This is similar to the commit cd2fd6eab480 ("platform/x86: int3472: Check for adev == NULL"). Add a check for adev not being set and return -ENODEV in that case to avoid a possible NULL pointer deref in int3402_thermal_probe(). Note, under the same directory, int3400_thermal_probe() has such a check. [rjw: Subject edit, added Fixes:] **CVE ID: CVE-2025-23136**	https://git.kernel.org/stable/c/0c49f12c77b77a706fd41370c11910635e491845, https://git.kernel.org/stable/c/2542a3f70e563a9e70e7ded314286535a3321bdb, https://git.kernel.org/stable/c/3155d5261b518776d1b807d9d922669991bbee56	O-LIN-LINU-050525/458
NULL Pointer Dereference	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: remoteproc: core: Clear table_sz when rproc_shutdown There is case as below could trigger kernel dump: Use U-Boot to start remote processor(rproc) with resource table	https://git.kernel.org/stable/c/068f6648ff5b0c7adeb6c363fae7fb188aa178fa, https://git.kernel.org/stable/c/2df19f5f6f72da6f6ebab7cdb3a3b9f7686bb476, https://git.kernel.org/stable/c/6e66bca8cd51e	O-LIN-LINU-050525/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			published to a fixed address by rproc. After Kernel boots up, stop the rproc, load a new firmware which doesn't have resource table ,and start rproc. When starting rproc with a firmware not have resource table, `memcpy(loaded_table, rproc->cached_table, rproc->table_sz)` will trigger dump, because rproc->cache_table is set to NULL during the last stop operation, but rproc->table_sz is still valid. This issue is found on i.MX8MP and i.MX9. Dump as below: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000096000004 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 user pgtable: 4k pages, 48-bit VAs, pgdp=000000010af63000 [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1]	bedd5d3242690 6a38e4a3c69c5f	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PREEMPT SMP Modules linked in: CPU: 2 UID: 0 PID: 1060 Comm: sh Not tainted 6.14.0-rc7-next-20250317-dirty #38 Hardware name: NXP i.MX8MPlus EVK board (DT) pstate: a0000005 (NzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __pi_memcpy_generic+0x110/0x22c lr : rproc_start+0x88/0x1e0 Call trace: __pi_memcpy_generic+0x110/0x22c (P) rproc_boot+0x198/0x57c state_store+0x40/0x104 dev_attr_store+0x18/0x2c sysfs_kf_write+0x7c/0x94 kernfs_fop_write_iter+0x120/0x1cc vfs_write+0x240/0x378 ksys_write+0x70/0x108 __arm64_sys_write+0x1c/0x28 invoke_syscall+0x48/0x10c el0_svc_common.constprop.0+0xc0/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x30/0xcc el0t_64_sync_handler+0x10c/0x138 el0t_64_sync+0x198/0x19c Clear rproc->table_sz to address the issue. **CVE ID: CVE-2025-38152**		
Improper Validation of Array Index	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: clk: samsung: Fix UBSAN	https://git.kernel.org/stable/c/00307934eb94aaa0a99addfb37b9fe206f945004	O-LIN-LINU-050525/460

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			panic in samsung_clk_init() With UBSAN_ARRAY_BOUNDS=y, I'm hitting the below panic due to dereferencing `ctx->clk_data.hws` before setting `ctx->clk_data.num = nr_clks`. Move that up to fix the crash. UBSAN: array index out of bounds: 00000000f2005512 [#1] PREEMPT SMP <snip> Call trace: samsung_clk_init+0x110/0x124 (P) samsung_clk_init+0x48/0x124 (L) samsung_cmu_register_one+0x3c/0xa0 exynos_arm64_register_cmu+0x54/0x64 __gs101_cmu_top_of_clk_init_declare+0x28/0x60 ... **CVE ID: CVE-2025-39728**	, https://git.kernel.org/stable/c/0fef48f4a70e45a93e73c39023c3a6ea624714d6 , https://git.kernel.org/stable/c/157de9e48007a20c65d02fc0229a16f38134a72d	
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: arm64: Don't call NULL in do_compat_alignment_fixup() do_alignment_t32_to_handler() only fixes up alignment faults for specific instructions; it returns NULL otherwise (e.g. LDREX). When	https://git.kernel.org/stable/c/2df8ee605eb6806cd41c2095306db05206633a08, https://git.kernel.org/stable/c/617a4b0084a547917669fef2b54253cc9c064990, https://git.kernel.org/stable/c/c28f31deeacda3	O-LIN-LINU-050525/461

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that's the case, signal to the caller that it needs to proceed with the regular alignment fault handling (i.e. SIGBUS). Without this patch, the kernel panics: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000086000006 EC = 0x21: IABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x06: level 2 translation fault user pgtable: 4k pages, 48-bit VAs, pgdp=00000800164aa000 [0000000000000000] pgd=0800081fdbd22003, p4d=0800081fdbd22003, pud=08000815d51c6003, pmd=0000000000000000 Internal error: Oops: 0000000086000006 [#1] SMP Modules linked in: cfg80211 rfkill xt_nat xt_tcpudp xt_conntrack nft_chain_nat xt_MASQUERADE nf_nat nf_conntrack_netlink nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 xfrm_user xfrm_algo xt_addrtype nft_compat br_netfilter veth nvme_fa> libcrc32c crc32c_generic raid0 multipath linear dm_mod dax raid1 md_mod xhci_pci nvme xhci_hcd nvme_core t10_pi usbcore igb crc64_rocksoft crc64 crc_t10dif crct10dif_generic crct10dif_ce crct10dif_common	07acfee2f18c0ad904e5123aac	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			usb_common i2c_algo_bit i2c> CPU: 2 PID: 3932954 Comm: WPEWebProcess Not tainted 6.1.0-31-arm64 #1 Debian 6.1.128-1 Hardware name: GIGABYTE MP32-AR1-00/MP32-AR1-00, BIOS F18v (SCP: 1.08.20211002) 12/01/2021 pstate: 80400009 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : 0x0 lr : do_compat_alignment_fixup +0xd8/0x3dc sp : ffff80000f973dd0 x29: ffff80000f973dd0 x28: ffff081b42526180 x27: 0000000000000000 x26: 0000000000000000 x25: 0000000000000000 x24: 0000000000000000 x23: 0000000000000004 x22: 0000000000000000 x21: 0000000000000001 x20: 00000000e8551f00 x19: ffff80000f973eb0 x18: 0000000000000000 x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : ffffaebc949bc488 x8 : 0000000000000000 x7 : 0000000000000000 x6 : 0000000000000000 x5 : 0000000000400000 x4 : 0000ffffffffffe x3 : 0000000000000000 x2 : ffff80000f973eb0 x1 : 00000000e8551f00 x0 : 0000000000000001 Call trace: 0x0		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_alignment_fault+0x40/0x50 do_mem_abort+0x4c/0xa0 el0_da+0x48/0xf0 el0t_32_sync_handler+0x110/0x140 el0t_32_sync+0x190/0x194 Code: bad PC value ---[end trace 0000000000000000]--- **CVE ID: CVE-2025-22033**		
NULL Pointer Dereference	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: arcnet: Add NULL check in com20020pci_probe() devm_kasprintf() returns NULL when memory allocation fails. Currently, com20020pci_probe() does not check for this case, which results in a NULL pointer dereference. Add NULL check after devm_kasprintf() to prevent this issue and ensure no resources are left allocated. **CVE ID: CVE-2025-22054**	https://git.kernel.org/stable/c/661cf5d102949898c931e81fd4e1c773afcdeafa, https://git.kernel.org/stable/c/887226163504494ea7e58033a97c2d2ab12e05d4, https://git.kernel.org/stable/c/905a34dc1ad9a53a8aaaf8a759ea5dbaaa30418d	O-LIN-LINU-050525/462
Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.24					
Use After Free	18-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: HSI: ssi_protocol: Fix use after free vulnerability in ssi_protocol Driver Due to Race Condition In the ssi_protocol_probe() function, &ssi->work is bound with ssip_xmit_work(), In	https://git.kernel.org/stable/c/4b4194c9a7a8f92db39e8e86c85f4fb12ebbec4f, https://git.kernel.org/stable/c/58eb29dba712ab0f13af59ca2fe545f5ce360e78, https://git.kernel.org/stable/c/834e602d0cc7c	O-LIN-LINU-050525/463

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ssip_pn_setup(), the ssip_pn_xmit() function within the ssip_pn_ops structure is capable of starting the work. If we remove the module which will call ssi_protocol_remove() to make a cleanup, it will free ssi through kfree(ssi), while the work mentioned above will be used. The sequence of operations that may lead to a UAF bug is as follows: CPU0 CPU1 | ssip_xmit_work ssi_protocol_remove | kfree(ssi); | | struct hsi_client *cl = ssi->cl; | // use ssi Fix it by ensuring that the work is canceled before proceeding with the cleanup in ssi_protocol_remove(). **CVE ID: CVE-2025-37838**	743bfce734fad4a46cefc0f9ab1	
Affected Version(s): From (including) 6.8 Up to (excluding) 6.12.23					
Improper Validation of Array Index	18-Apr-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: iio: light: Add check for array bounds in veml6075_read_int_time_ms The array contains only 5 elements, but the index calculated by veml6075_read_int_time_index can range from 0 to 7, which could lead to out-of-	https://git.kernel.org/stable/c/18a08b5632809faa671279b3cd27d5f96cc5a3f0, https://git.kernel.org/stable/c/7a40b52d4442178bee0cf1c36bc450ab951cef0f, https://git.kernel.org/stable/c/9c40a68b7f97fa487e6c7e67fcf4f	O-LIN-LINU-050525/464

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds access. The check prevents this issue. Coverity Issue CID 1574309: (#1 of 1): Out-of-bounds read (OVERRUN) overrun-local: Overrunning array veml6075_it_ms of 5 4-byte elements at element index 7 (byte offset 31) using index int_index (which evaluates to 7) This is hardening against potentially broken hardware. Good to have but not necessary to backport. **CVE ID: CVE-2025-40114**	846a1f96692	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Apr-2025	7	In the Linux kernel, the following vulnerability has been resolved: exfat: fix random stack corruption after get_block When get_block is called with a buffer_head allocated on the stack, such as do_mpage_readpage, stack corruption due to buffer_head UAF may occur in the following race condition situation. <CPU 0> <CPU 1> mpage_read_folio <<bh on stack>> do_mpage_readpage exfat_get_block bh_read __bh_read get_bh(bh) submit_bh wait_on_buffer ...	https://git.kernel.org/stable/c/1bb7ff4204b6d4927e982cd256286c09ed4fd8ca, https://git.kernel.org/stable/c/49b0a6ab8e528a0c1c50e37cef9b9c7c121365f2, https://git.kernel.org/stable/c/f7447286363dc1e410bf30b87d75168f3519f9cc	O-LIN-LINU-050525/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			end_buffer_read_sync __end_buffer_read_notouch unlock_buffer <<keep going>> ... ... <<bh is not valid out of mpage_read_folio>> . . another_function <<variable A on stack>> put_bh(bh) atomic_dec(bh->b_count) * stack corruption here * This patch returns -EAGAIN if a folio does not have buffers when bh_read needs to be called. By doing this, the caller can fallback to functions like block_read_full_folio(), create a buffer_head in the folio, and then call get_block again. Let's do not call bh_read() with on-stack buffer_head. **CVE ID: CVE-2025-22036**		
Affected Version(s): From (including) 6.9 Up to (excluding) 6.12.23					
Improper Locking	16-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: ALSA: timer: Don't take register_mutex with copy_from/to_user() The infamous mmap_lock taken in copy_from/to_user() can be often	https://git.kernel.org/stable/c/15291b561d8cc835a2eea76b394070cf8e072771, https://git.kernel.org/stable/c/296f7a9e15aab276db11206cbc1e2ae1215d7862,	O-LIN-LINU-050525/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			problematic when it's called inside another mutex, as they might lead to deadlocks. In the case of ALSA timer code, the bad pattern is with guard(mutex)(&register_mutex) that covers copy_from/to_user() -- which was mistakenly introduced at converting to guard(), and it had been carefully worked around in the past. This patch fixes those pieces simply by moving copy_from/to_user() out of the register mutex lock again. **CVE ID: CVE-2025-23134**	https://git.kernel.org/stable/c/3424c8f53bc63c87712a7fc22dc13d0cc85fb0d6	
NULL Pointer Dereference	18-Apr-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: x86/resctrl: Fix allocation of cleanest CLOSID on platforms with no monitors Commit 6eac36bb9eb0 ("x86/resctrl: Allocate the cleanest CLOSID by searching closid_num_dirty_rmid") added logic that causes resctrl to search for the CLOSID with the fewest dirty cache lines when creating a new control group, if requested by the arch code. This depends on the values read from the llc_occupancy counters. The logic is	https://git.kernel.org/stable/c/93a418fc61da13d1ee4047d4d1327990f7a2816a, https://git.kernel.org/stable/c/a121798ae669351ec0697c94f71c3a692b2a755b, https://git.kernel.org/stable/c/a8a1bcc27d4607227088d80483164289b5348293	O-LIN-LINU-050525/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applicable to architectures where the CLOSID effectively forms part of the monitoring identifier and so do not allow complete freedom to choose an unused monitoring identifier for a given CLOSID. This support missed that some platforms may not have these counters. This causes a NULL pointer dereference when creating a new control group as the array was not allocated by dom_data_init(). As this feature isn't necessary on platforms that don't have cache occupancy monitors, add this to the check that occurs when a new control group is allocated. **CVE ID: CVE-2025-38049**		
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
N/A	25-Apr-2025	8.8	Commvault Web Server has an unspecified vulnerability that can be exploited by a remote, authenticated attacker. According to the Commvault advisory: "Webservers can be compromised through bad actors creating and executing webshells." Fixed in version 11.36.46, 11.32.89, 11.28.141, and 11.20.217 for Windows and Linux platforms. This vulnerability was added to the CISA Known Exploited Vulnerabilities (KEV) Catalog on 2025-04-28.	https://documentation.commvault.com/securityadvisories/CV_2025_03_1.html, https://www.commvault.com/blogs/notice-security-advisory-update, https://www.commvault.com/blogs/security-advisory-march-7-2025	O-MIC-WIND-050525/468

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-3928		
Vendor: Netgear					
Product: r6100_firmware					
Affected Version(s): 1.0.1.28					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Apr-2025	9.8	Buffer Overflow vulnerability in Netgear-R61 router V1.0.1.28 allows a remote attacker to execute arbitrary code via the QUERY_STRING key value **CVE ID: CVE-2025-29044**	N/A	O-NET-R610-050525/469
Vendor: Tenda					
Product: ac10_firmware					
Affected Version(s): 16.03.10.20					
Stack-based Buffer Overflow	17-Apr-2025	7.5	Tenda AC10 V4.0si_V16.03.10.20 is vulnerable to Buffer Overflow in AdvSetMacMtuWan via cloneType2. **CVE ID: CVE-2025-25457**	N/A	O-TEN-AC10-050525/470
Stack-based Buffer Overflow	17-Apr-2025	7.5	Tenda AC10 V4.0si_V16.03.10.20 is vulnerable to Buffer Overflow in AdvSetMacMtuWan via wanSpeed2. **CVE ID: CVE-2025-25454**	N/A	O-TEN-AC10-050525/471
Stack-based Buffer Overflow	17-Apr-2025	7.5	Tenda AC10 V4.0si_V16.03.10.20 is vulnerable to Buffer Overflow in AdvSetMacMtuWan via wanMTU2. **CVE ID: CVE-2025-25455**	N/A	O-TEN-AC10-050525/472
Product: ac15_firmware					
Affected Version(s): 15.03.05.19					
Improper Restriction of	18-Apr-2025	8.8	A vulnerability was found in Tenda AC15 up to 15.03.05.19 and classified	N/A	O-TEN-AC15-050525/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			as critical. This issue affects the function fromSetWirelessRepeat of the file /goform/WifiExtraSet. The manipulation of the argument mac leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3786**		
Product: ac9_firmware					
Affected Version(s): 15.03.05.14_multi					
Stack-based Buffer Overflow	23-Apr-2025	9.8	In the Tenda ac9 v1.0 router with firmware V15.03.05.14_multi, there is a stack overflow vulnerability in /goform/WifiWpsStart, which may lead to remote arbitrary code execution. **CVE ID: CVE-2025-45429**	N/A	O-TEN-AC9_-050525/474
Stack-based Buffer Overflow	23-Apr-2025	9.8	In Tenda ac9 v1.0 with firmware V15.03.05.14_multi, the rebootTime parameter of /goform/SetSysAutoRebbotCfg has a stack overflow vulnerability, which can lead to remote arbitrary code execution. **CVE ID: CVE-2025-45428**	N/A	O-TEN-AC9_-050525/475
Stack-based Buffer Overflow	23-Apr-2025	9.8	In Tenda AC9 v1.0 with firmware V15.03.05.14_multi, the security parameter of /goform/WifiBasicSet has a stack overflow vulnerability, which can lead to remote arbitrary code execution. **CVE ID: CVE-2025-45427**	N/A	O-TEN-AC9_-050525/476
Vendor: think					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: tk-rt-wr135g_firmware					
Affected Version(s): 3.0.2-x000					
Reliance on Cookies without Validation and Integrity Checking	17-Apr-2025	8.4	An issue in Think Router Tk-Rt-Wr135G V3.0.2-X000 allows attackers to bypass authentication via a crafted cookie. **CVE ID: CVE-2024-55211**	N/A	O-THI-TK-R-050525/477
Vendor: totolink					
Product: a3000ru_firmware					
Affected Version(s): 5.9c.5185_b20201128					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth remote command execution vulnerability in the NTPSyncWithHost function through the hostTime parameter. **CVE ID: CVE-2025-28034**	N/A	O-TOT-A300-050525/478
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A830R V4.1.2cu.5182_B20201102 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28035**	N/A	O-TOT-A300-050525/479
Improper Neutralization of Special Elements used in an OS	22-Apr-2025	9.8	TOTOLINK A950RG V4.1.2cu.5161_B20200903 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function	N/A	O-TOT-A300-050525/480

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			through the NoticeUrl parameter. **CVE ID: CVE-2025-28036**		
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpForm parameter. **CVE ID: CVE-2025-28032**	N/A	O-TOT-A300-050525/481
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpTo parameter. **CVE ID: CVE-2025-28033**	N/A	O-TOT-A300-050525/482
Product: a3100r_firmware					
Affected Version(s): 4.1.2cu.5247_b20211129					
Improper Neutralization of Special Elements used in an	22-Apr-2025	9.8	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R	N/A	O-TOT-A310-050525/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth remote command execution vulnerability in the NTPSyncWithHost function through the hostTime parameter. **CVE ID: CVE-2025-28034**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A830R V4.1.2cu.5182_B20201102 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28035**	N/A	O-TOT-A310-050525/484
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A950RG V4.1.2cu.5161_B20200903 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28036**	N/A	O-TOT-A310-050525/485
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpForm	N/A	O-TOT-A310-050525/486

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter. **CVE ID: CVE-2025-28032**		
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpTo parameter. **CVE ID: CVE-2025-28033**	N/A	O-TOT-A310-050525/487
Product: a3700r_firmware					
Affected Version(s): 9.1.2u.5822_b20200513					
Incorrect Privilege Assignment	16-Apr-2025	5.3	A vulnerability was found in TOTOLINK A3700R 9.1.2u.5822_B20200513. It has been declared as critical. Affected by this vulnerability is the function setUrlFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-3674**	N/A	O-TOT-A370-050525/488
Product: a800r_firmware					
Affected Version(s): 4.1.2cu.5137_b20200730					
Improper Neutralization of Special Elements used in an OS	22-Apr-2025	9.8	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102,	N/A	O-TOT-A800-050525/489

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth remote command execution vulnerability in the NTPSyncWithHost function through the hostTime parameter. **CVE ID: CVE-2025-28034**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A830R V4.1.2cu.5182_B20201102 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28035**	N/A	O-TOT-A800-050525/490
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A950RG V4.1.2cu.5161_B20200903 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28036**	N/A	O-TOT-A800-050525/491
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpForm parameter.	N/A	O-TOT-A800-050525/492

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-28032		
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpTo parameter. **CVE ID: CVE-2025-28033**	N/A	O-TOT-A800-050525/493
Product: a810r_firmware					
Affected Version(s): 4.1.2cu.5182_b20201026					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A810R V4.1.2cu.5182_B20201026 and A950RG V4.1.2cu.5161_B20200903 were found to contain a pre-auth remote command execution vulnerability in the setDiagnosisCfg function through the ipDomain parameter. **CVE ID: CVE-2025-28037**	N/A	O-TOT-A810-050525/494
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth remote command	N/A	O-TOT-A810-050525/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution vulnerability in the NTPSyncWithHost function through the hostTime parameter. **CVE ID: CVE-2025-28034**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Apr-2025	9.8	TOTOLINK A810R V4.1.2cu.5182_B20201026 was found to contain a buffer overflow vulnerability in the cstecgi.cgi **CVE ID: CVE-2025-28024**	N/A	O-TOT-A810-050525/496
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A950RG V4.1.2cu.5161_B20200903 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28036**	N/A	O-TOT-A810-050525/497
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A830R V4.1.2cu.5182_B20201102 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28035**	N/A	O-TOT-A810-050525/498
Stack-based Buffer Overflow	22-Apr-2025	8.8	TOTOLINK A810R V4.1.2cu.5182_B20201026 was discovered to contain a stack overflow via the startTime and endTime parameters in setParentalRules function. **CVE ID: CVE-2025-28030**	N/A	O-TOT-A810-050525/499
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903,	N/A	O-TOT-A810-050525/500

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpForm parameter. **CVE ID: CVE-2025-28032**		
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpTo parameter. **CVE ID: CVE-2025-28033**	N/A	O-TOT-A810-050525/501
Use of Hard-coded Password	22-Apr-2025	6.5	TOTOLINK A810R V4.1.2cu.5182_B20201026 was discovered to contain a hardcoded password for the telnet service in product.ini. **CVE ID: CVE-2025-28031**	N/A	O-TOT-A810-050525/502
Product: a830r_firmware					
Affected Version(s): 4.1.2cu.5182_b20201102					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128,	N/A	O-TOT-A830-050525/503

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth remote command execution vulnerability in the NTPSyncWithHost function through the hostTime parameter. **CVE ID: CVE-2025-28034**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A830R V4.1.2cu.5182_B20201102 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28035**	N/A	O-TOT-A830-050525/504
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A950RG V4.1.2cu.5161_B20200903 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28036**	N/A	O-TOT-A830-050525/505
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpForm parameter. **CVE ID: CVE-2025-28032**	N/A	O-TOT-A830-050525/506
Stack-based Buffer	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730,	N/A	O-TOT-A830-050525/507

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow			A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpTo parameter. **CVE ID: CVE-2025-28033**		
Product: a950rg_firmware					
Affected Version(s): 4.1.2cu.5161_b20200903					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth remote command execution vulnerability in the NTPSyncWithHost function through the hostTime parameter. **CVE ID: CVE-2025-28034**	N/A	O-TOT-A950-050525/508
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A830R V4.1.2cu.5182_B20201102 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28035**	N/A	O-TOT-A950-050525/509

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK A950RG V4.1.2cu.5161_B20200903 was found to contain a pre-auth remote command execution vulnerability in the setNoticeCfg function through the NoticeUrl parameter. **CVE ID: CVE-2025-28036**	N/A	O-TOT-A950-050525/510
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpForm parameter. **CVE ID: CVE-2025-28032**	N/A	O-TOT-A950-050525/511
Stack-based Buffer Overflow	22-Apr-2025	7.3	TOTOLINK A800R V4.1.2cu.5137_B20200730, A810R V4.1.2cu.5182_B20201026, A830R V4.1.2cu.5182_B20201102, A950RG V4.1.2cu.5161_B20200903, A3000RU V5.9c.5185_B20201128, and A3100R V4.1.2cu.5247_B20211129 were found to contain a pre-auth buffer overflow vulnerability in the setNoticeCfg function through the IpTo parameter. **CVE ID: CVE-2025-28033**	N/A	O-TOT-A950-050525/512
Affected Version(s): 4.1.2cu.5182_b20201026					
Improper	22-Apr-2025	9.8	TOTOLINK A810R	N/A	O-TOT-A950-

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			V4.1.2cu.5182_B20201026 and A950RG V4.1.2cu.5161_B20200903 were found to contain a pre-auth remote command execution vulnerability in the setDiagnosisCfg function through the ipDomain parameter. **CVE ID: CVE-2025-28037**		050525/513
Product: ex1200t_firmware					
Affected Version(s): 4.1.2cu.5232_b20210713					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK EX1200T V4.1.2cu.5232_B20210713 was found to contain a pre-auth remote command execution vulnerability in the setUpgradeFW function through the FileName parameter. **CVE ID: CVE-2025-28039**	N/A	O-TOT-EX12-050525/514
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2025	9.8	TOTOLINK EX1200T V4.1.2cu.5232_B20210713 was found to contain a pre-auth remote command execution vulnerability in the setWebWlanIdx function through the webWlanIdx parameter. **CVE ID: CVE-2025-28038**	N/A	O-TOT-EX12-050525/515
Product: x18_firmware					
Affected Version(s): 9.1.0cu.2024_b20220329					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Apr-2025	9.8	TOTOLINK X18 v9.1.0cu.2024_B20220329 has an unauthorized arbitrary command execution in the enable parameter' of the sub_41105C function of cstecgi .cgi. **CVE ID: CVE-2025-29209**	N/A	O-TOT-X18_-050525/516
Vendor: Tp-link					
Product: eap120_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2025	7.3	SQL Injection vulnerability exists in the TP-Link EAP120 router s login dashboard (version 1.0), allowing an unauthenticated attacker to inject malicious SQL statements via the login fields. NOTE: this is disputed because the issue can only be reproduced on a supplier-provided emulator, where access control is intentionally absent for ease of functional testing. **CVE ID: CVE-2025-29648**	N/A	O-TP--EAP1-050525/517
Product: m7000_firmware					
Affected Version(s): 1.0.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2025	9.8	SQL Injection vulnerability exists in the TP-Link M7000 4G LTE Mobile Wi-Fi Router Firmware Version: 1.0.7 Build 180127 Rel.55998n, allowing an unauthenticated attacker to inject malicious SQL statements via the username and password fields. NOTE: this is disputed because the issue can only be reproduced on a supplier-provided emulator, where access control is intentionally absent for ease of functional testing. **CVE ID: CVE-2025-29652**	N/A	O-TP--M700-050525/518
Product: m7200_firmware					
Affected Version(s): 1.0.7					
Improper Neutralization of Special Elements used in an SQL Command	16-Apr-2025	6.3	SQL Injection vulnerability exists in the TP-Link M7200 4G LTE Mobile Wi-Fi Router Firmware Version: 1.0.7 Build 180127 Rel.55998n, allowing an unauthenticated attacker to	N/A	O-TP--M720-050525/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			inject malicious SQL statements via the username and password fields. NOTE: this is disputed because the issue can only be reproduced on a supplier-provided emulator, where access control is intentionally absent for ease of functional testing. **CVE ID: CVE-2025-29650**		
Product: m7450_firmware					
Affected Version(s): 1.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2025	9.8	SQL Injection vulnerability exists in the TP-Link M7450 4G LTE Mobile Wi-Fi Router Firmware Version: 1.0.2 Build 170306 Rel.1015n, allowing an unauthenticated attacker to inject malicious SQL statements via the username and password fields. **CVE ID: CVE-2025-29653**	N/A	O-TP--M745-050525/520
Product: m7650_firmware					
Affected Version(s): 1.0.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2025	9.8	SQL Injection vulnerability exists in the TP-Link M7650 4G LTE Mobile Wi-Fi Router Firmware Version: 1.0.7 Build 170623 Rel.1022n, allowing an unauthenticated attacker to inject malicious SQL statements via the username and password fields. NOTE: this is disputed because the issue can only be reproduced on a supplier-provided emulator, where access control is intentionally absent for ease of functional testing. **CVE ID: CVE-2025-29651**	N/A	O-TP--M765-050525/521

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: tl-wr840n_firmware					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2025	7.3	SQL Injection vulnerability exists in the TP-Link TL-WR840N router s login dashboard (version 1.0), allowing an unauthenticated attacker to inject malicious SQL statements via the username and password fields. NOTE: this is disputed because the issue can only be reproduced on a supplier-provided emulator, where access control is intentionally absent for ease of functional testing. **CVE ID: CVE-2025-29649**	N/A	O-TP--TL-W-050525/522