National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Sep 2019 Vol. 06 No. 17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
10web					
photo_gallery					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-09-2019	4.3	Cross site scripting (XSS) in the photo-gallery (10Web Photo Gallery) plugin before 1.5.35 for WordPress exists via admin/models/Galleries.php. **CVE ID : CVE-2019-16117**	N/A	A-10W-PHOT-230919/1
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-09-2019	4.3	Cross site scripting (XSS) in the photo-gallery (10Web Photo Gallery) plugin before 1.5.35 for WordPress exists via admin/controllers/Options.php. **CVE ID : CVE-2019-16118**	N/A	A-10W-PHOT-230919/2
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-09-2019	7.5	SQL injection in the photo-gallery (10Web Photo Gallery) plugin before 1.5.35 for WordPress exists via the admin/controllers/Albumsgalleries.php album_id parameter. **CVE ID : CVE-2019-16119**	N/A	A-10W-PHOT-230919/3
Adobe					
application_manager					
Untrusted Search Path	12-09-2019	6.8	Adobe application manager installer version 10.0 have an Insecure Library Loading (DLL hijacking) vulnerability.	https://helpx.adobe.com/security/products/appli	A-ADO-APPL-230919/4

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation could lead to Arbitrary Code Execution in the context of the current user. **CVE ID : CVE-2019-8076**	cation_manager/apsb19-45.html	
flash_player					
Origin Validation Error	12-09-2019	10	Adobe Flash Player 32.0.0.238 and earlier versions, 32.0.0.207 and earlier versions have a Same Origin Method Execution vulnerability. Successful exploitation could lead to Arbitrary Code Execution in the context of the current user. **CVE ID : CVE-2019-8069**	https://helpx.adobe.com/security/products/flash-player/apsb19-46.html	A-ADO-FLAS-230919/5
Use After Free	12-09-2019	10	Adobe Flash Player 32.0.0.238 and earlier versions, 32.0.0.207 and earlier versions have a Use after free vulnerability. Successful exploitation could lead to Arbitrary Code Execution in the context of the current user. **CVE ID : CVE-2019-8070**	https://helpx.adobe.com/security/products/flash-player/apsb19-46.html	A-ADO-FLAS-230919/6
flash_player_desktop_runtime					
Origin Validation Error	12-09-2019	10	Adobe Flash Player 32.0.0.238 and earlier versions, 32.0.0.207 and earlier versions have a Same Origin Method Execution vulnerability. Successful exploitation could lead to Arbitrary Code Execution in the context of the current user.	https://helpx.adobe.com/security/products/flash-player/apsb19-46.html	A-ADO-FLAS-230919/7

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8069		
Use After Free	12-09-2019	10	Adobe Flash Player 32.0.0.238 and earlier versions, 32.0.0.207 and earlier versions have a Use after free vulnerability. Successful exploitation could lead to Arbitrary Code Execution in the context of the current user. **CVE ID : CVE-2019-8070**	https://helpx.adobe.com/security/products/flash-player/apsb19-46.html	A-ADO-FLAS-230919/8
Advantech					
webaccess					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-09-2019	7.5	Stack-based buffer overflow in Advantech WebAccess/SCADA 8.4.1 allows a remote, unauthenticated attacker to execute arbitrary code via a crafted IOCTL 70603 RPC message. **CVE ID : CVE-2019-3975**	N/A	A-ADV-WEBA-230919/9
Afterlogic					
aurora					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-09-2019	4.3	Afterlogic Aurora through 8.3.9-build-a3 has XSS that can be leveraged for session hijacking by retrieving the session cookie from the administrator login. **CVE ID : CVE-2019-16238**	N/A	A-AFT-AURO-230919/10
airbrake					
airbrake_ruby					
N/A	06-09-2019	5	The Airbrake Ruby notifier 4.2.3 for Airbrake mishandles the blacklist_keys	N/A	A-AIR-AIRB-230919/11

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration option and consequently may disclose passwords to unauthorized actors. This is fixed in 4.2.4 (also, 4.2.2 and earlier are unaffected). **CVE ID : CVE-2019-16060**		
Alfresco					
alfresco					
N/A	05-09-2019	7.5	An issue was discovered in Alfresco Community Edition versions 6.0 and lower. An unauthenticated, remote attacker could authenticate to Alfresco's Solr Web Admin Interface. The vulnerability is due to the presence of a default private key that is present in all default installations. An attacker could exploit this vulnerability by using the extracted private key and bundling it into a PKCS12. A successful exploit could allow the attacker to gain information about the target system (e.g., OS type, system file locations, Java version, Solr version, etc.) as well as the ability to launch further attacks by leveraging the access to Alfresco's Solr Web Admin Interface. **CVE ID : CVE-2019-14222**	N/A	A-ALF-ALFR-230919/12
URL Redirection to Untrusted Site ('Open	06-09-2019	5.8	An issue was discovered in Alfresco Community Edition versions below 5.2.6, 6.0.N and 6.1.N. The Alfresco Share	N/A	A-ALF-ALFR-230919/13

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redirect')			application is vulnerable to an Open Redirect attack via a crafted POST request. By manipulating the POST parameters, an attacker can redirect a victim to a malicious website over any protocol the attacker desires (e.g.,http, https, ftp, smb, etc.). **CVE ID : CVE-2019-14223**		
Improper Input Validation	05-09-2019	9	An issue was discovered in Alfresco Community Edition 5.2 201707. By leveraging multiple components in the Alfresco Software applications, an exploit chain was observed that allows an attacker to achieve remote code execution on the victim machine. The attacker must upload malicious Solr configuration files and then receive a JMX connection from the victim, and serve a Java object that results in deserialization and code execution. **CVE ID : CVE-2019-14224**	N/A	A-ALF-ALFR-230919/14
Apache					
ofbiz					
Deserialization of Untrusted Data	11-09-2019	7.5	The java.io.ObjectInputStream is known to cause Java serialisation issues. This issue here is exposed by the "webtools/control/httpService" URL, and uses Java deserialization to perform	N/A	A-APA-OFBI-230919/15

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution. In the HttpEngine, the value of the request parameter "serviceContext" is passed to the "deserialize" method of "XmlSerializer". Apache Ofbiz is affected via two different dependencies: "commons-beanutils" and an out-dated version of "commons-fileupload" Mitigation: Upgrade to 16.11.06 or manually apply the commits from OFBIZ-10770 and OFBIZ-10837 on branch 16 **CVE ID : CVE-2019-0189**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	4.3	The "Blog", "Forum", "Contact Us" screens of the template "ecommerce" application bundled in Apache OFBiz are weak to Stored XSS attacks. Mitigation: Upgrade to 16.11.06 or manually apply the following commits on branch 16.11: 1858438, 1858543, 1860595 and 1860616 **CVE ID : CVE-2019-10073**	N/A	A-APA-OFBI-230919/16
Improper Input Validation	11-09-2019	7.5	An RCE is possible by entering Freemarker markup in an Apache OFBiz Form Widget textarea field when encoding has been disabled on such a field. This was the case for the Customer Request "story" input in the Order Manager application. Encoding should not be disabled without good reason	N/A	A-APA-OFBI-230919/17

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and never within a field that accepts user input. Mitigation: Upgrade to 16.11.06 or manually apply the following commit on branch 16.11: r1858533 **CVE ID : CVE-2019-10074**		
solr					
Uncontrolled Resource Consumption	10-09-2019	5	Solr versions 1.3.0 to 1.4.1, 3.1.0 to 3.6.2 and 4.0.0 to 4.10.4 are vulnerable to an XML resource consumption attack (a.k.a. Lol Bomb) via it?s update handler.?By leveraging XML DOCTYPE and ENTITY type elements, the attacker can create a pattern that will expand when the server parses the XML causing OOMs. **CVE ID : CVE-2019-12401**	N/A	A-APA-SOLR-230919/18
traffic_control					
Improper Authentication	09-09-2019	6.8	Improper authentication is possible in Apache Traffic Control versions 3.0.0 and 3.0.1 if LDAP is enabled for login in the Traffic Ops API component. Given a username for a user that can be authenticated via LDAP, it is possible to improperly authenticate as that user without that user's correct password. **CVE ID : CVE-2019-12405**	N/A	A-APA-TRAF-230919/19
Artifex					
ghostscript					
N/A	03-09-2019	6.8	A flaw was found in,	N/A	A-ART-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ghostscript versions prior to 9.28, in the .pdf_hook_DSC_Creator procedure where it did not properly secure its privileged calls, enabling scripts to bypass `-dSAFER` restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands. **CVE ID : CVE-2019-14811**		GHOS-230919/20
N/A	06-09-2019	7.5	A flaw was found in ghostscript, versions 9.x before 9.28, in the setsystemparams procedure where it did not properly secure its privileged calls, enabling scripts to bypass `-dSAFER` restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands. **CVE ID : CVE-2019-14813**	N/A	A-ART-GHOS-230919/21
Asus					
precision_touchpad					
N/A	04-09-2019	7.5	AsusPTPFilter.sys on Asus Precision TouchPad 11.0.0.25 hardware has a Pool Overflow associated with the \\.\AsusTP device, leading to a DoS or potentially privilege escalation via a crafted DeviceIoControl call. **CVE ID : CVE-2019-10709**	N/A	A-ASU-PREC-230919/22

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Atlassian					
jira					
Incorrect Default Permissions	11-09-2019	5	The /rest/api/1.0/render resource in Jira before version 8.4.0 allows remote anonymous attackers to determine if an attachment with a specific name exists and if an issue key is valid via a missing permissions check. **CVE ID : CVE-2019-14995**	N/A	A-ATL-JIRA-230919/23
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	4.3	The FilterPickerPopup.jspa resource in Jira before version 7.13.7, and from version 8.0.0 before version 8.3.3 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the searchOwnerUserName parameter. **CVE ID : CVE-2019-14996**	N/A	A-ATL-JIRA-230919/24
Information Exposure	11-09-2019	4.3	The AccessLogFilter class in Jira before version 8.4.0 allows remote anonymous attackers to learn details about other users, including their username, via an information expose through caching vulnerability when Jira is configured with a reverse Proxy and or a load balancer with caching or a CDN. **CVE ID : CVE-2019-14997**	N/A	A-ATL-JIRA-230919/25
Cross-Site Request Forgery	11-09-2019	4.3	The Webwork action Cross-Site Request Forgery (CSRF) protection implementation in	N/A	A-ATL-JIRA-230919/26

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			Jira before version 8.4.0 allows remote attackers to bypass its protection via "cookie tossing" a CSRF cookie from a subdomain of a Jira instance. **CVE ID : CVE-2019-14998**		
Information Exposure	11-09-2019	5	The /rest/api/latest/groupuserpicker resource in Jira before version 8.4.0 allows remote attackers to enumerate usernames via an information disclosure vulnerability. **CVE ID : CVE-2019-8449**	N/A	A-ATL-JIRA-230919/27
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	3.5	Various templates of the Optimization plugin in Jira before version 7.13.6, and from version 8.0.0 before version 8.4.0 allow remote attackers who have permission to manage custom fields to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the name of a custom field. **CVE ID : CVE-2019-8450**	N/A	A-ATL-JIRA-230919/28
Server-Side Request Forgery (SSRF)	11-09-2019	6.4	The /plugins/servlet/gadgets/makeRequest resource in Jira before version 8.4.0 allows remote attackers to access the content of internal network resources via a Server Side Request Forgery (SSRF) vulnerability due to a logic bug in the JiraWhitelist	N/A	A-ATL-JIRA-230919/29

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			class. **CVE ID : CVE-2019-8451**		
Atutor					
atutor					
Improper Access Control	09-09-2019	7.5	In ATutor 2.2.4, an unauthenticated attacker can change the application settings and force it to use his crafted database, which allows him to gain access to the application. Next, he can change the directory that the application uploads files to, which allows him to achieve remote code execution. This occurs because install/include/header.php does not restrict certain changes (to db_host, db_login, db_password, and content_dir) within install/include/step5.php. **CVE ID : CVE-2019-16114**	N/A	A-ATU-ATUT-230919/30
Bitcoin					
bitcoin_core					
Inadequate Encryption Strength	05-09-2019	5	In Bitcoin Core 0.18.0, bitcoin-qt stores wallet.dat data unencrypted in memory. Upon a crash, it may dump a core file. If a user were to mishandle a core file, an attacker can reconstruct the user's wallet.dat file, including their private keys, via a grep "6231 0500" command. **CVE ID : CVE-2019-15947**	N/A	A-BIT-BITC-230919/31
blake2					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
blake2					
Improper Input Validation	09-09-2019	7.5	An issue was discovered in the blake2 crate before 0.8.1 for Rust. The BLAKE2b and BLAKE2s algorithms, when used with HMAC, produce incorrect results because the block sizes are half of the required sizes. **CVE ID : CVE-2019-16143**	N/A	A-BLA-BLAK-230919/32
bludit					
bludit					
Improper Control of Generation of Code ('Code Injection')	08-09-2019	6.5	Bludit 3.9.2 allows remote code execution via bl-kernel/ajax/upload-images.php because PHP code can be entered with a .jpg file name, and then this PHP code can write other PHP code to a ../ pathname. **CVE ID : CVE-2019-16113**	N/A	A-BLU-BLUD-230919/33
Blynk					
blynk-library					
Information Exposure	05-09-2019	5	An exploitable information disclosure vulnerability exists in the packet-parsing functionality of Blynk-Library v0.6.1. A specially crafted packet can cause an unterminated strncpy, resulting in information disclosure. An attacker can send a packet to trigger this vulnerability. **CVE ID : CVE-2019-5065**	N/A	A-BLY-BLYN-230919/34
bosch					
access					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	12-09-2019	4	An unauthenticated attacker can achieve unauthorized access to sensitive data by exploiting Windows SMB protocol on a client installation. With Bosch Access Professional Edition (APE) 3.8, client installations need to be authorized by the APE administrator. **CVE ID : CVE-2019-11899**	https://psirt.bosch.com/Advisory/BOSCH-SA-844044.html	A-BOS-ACCE-230919/35
Broadcom					
ca_client_automation					
Improper Access Control	06-09-2019	7.5	An access vulnerability in CA Common Services DIA of CA Technologies Client Automation 14 and Workload Automation AE 11.3.5, 11.3.6 allows a remote attacker to execute arbitrary code. **CVE ID : CVE-2019-13656**	N/A	A-BRO-CA_C-230919/36
ca_workload_automation_ae					
Improper Access Control	06-09-2019	7.5	An access vulnerability in CA Common Services DIA of CA Technologies Client Automation 14 and Workload Automation AE 11.3.5, 11.3.6 allows a remote attacker to execute arbitrary code. **CVE ID : CVE-2019-13656**	N/A	A-BRO-CA_W-230919/37
Canon					
print					
Information Exposure	05-09-2019	4.3	The ContentProvider in the Canon PRINT jp.co.canon.bsd.ad.pixmaprint 2.5.5 application for Android does not properly restrict	N/A	A-CAN-PRIN-230919/38

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			canon.ij.printer.capability.data data access. This allows an attacker's malicious application to obtain sensitive information including factory passwords for the administrator web interface and WPA2-PSK key. **CVE ID : CVE-2019-14339**		
carspot_project					
carspot					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-09-2019	3.5	The CarSpot theme before 2.1.7 for WordPress has stored XSS via the Phone Number field. **CVE ID : CVE-2019-15870**	N/A	A-CAR-CARS-230919/39
centos-webpanel					
centos_web_panel					
Authorization Bypass Through User-Controlled Key	10-09-2019	5.5	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.851, an insecure object reference allows an attacker to remove a target user from phpMyAdmin via an attacker account. **CVE ID : CVE-2019-14721**	N/A	A-CEN-CENT-230919/40
Improper Input Validation	10-09-2019	4	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.851, an insecure object reference allows an attacker to delete an e-mail forwarding destination from a victim's account via an attacker account. **CVE ID : CVE-2019-14722**	N/A	A-CEN-CENT-230919/41

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	10-09-2019	4	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.851, an insecure object reference allows an attacker to delete a victim's e-mail account via an attacker account. **CVE ID : CVE-2019-14723**	N/A	A-CEN-CENT-230919/42
Authorization Bypass Through User-Controlled Key	11-09-2019	5	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.851, an insecure object reference allows an attacker to edit an e-mail forwarding destination of a victim's account via an attacker account. **CVE ID : CVE-2019-14724**	N/A	A-CEN-CENT-230919/43
Authorization Bypass Through User-Controlled Key	11-09-2019	4	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.851, an insecure object reference allows an attacker to change the e-mail usage value of a victim account via an attacker account. **CVE ID : CVE-2019-14725**	N/A	A-CEN-CENT-230919/44
Improper Input Validation	10-09-2019	6.5	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.851, an insecure object reference allows an attacker to access and delete DNS records of a victim's account via an attacker account. **CVE ID : CVE-2019-14726**	N/A	A-CEN-CENT-230919/45
Improper Input Validation	10-09-2019	4	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.851, an insecure object reference allows an attacker to change the e-mail password of a victim account	N/A	A-CEN-CENT-230919/46

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via an attacker account. **CVE ID : CVE-2019-14727**		
Improper Input Validation	10-09-2019	4	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.851, an insecure object reference allows an attacker to add an e-mail forwarding destination to a victim's account via an attacker account. **CVE ID : CVE-2019-14728**	N/A	A-CEN-CENT-230919/47
Improper Input Validation	10-09-2019	5.5	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.851, an insecure object reference allows an attacker to delete a sub-domain from a victim's account via an attacker account. **CVE ID : CVE-2019-14729**	N/A	A-CEN-CENT-230919/48
Improper Input Validation	10-09-2019	4	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.851, an insecure object reference allows an attacker to delete a domain from a victim's account via an attacker account. **CVE ID : CVE-2019-14730**	N/A	A-CEN-CENT-230919/49
Cisco					
network_level_service					
N/A	04-09-2019	5	A vulnerability in the &ldquo;plug-and-play&rdquo; services component of Cisco Industrial Network Director (IND) could allow an unauthenticated, remote attacker to access sensitive information on an affected	N/A	A-CIS-NETW-230919/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability is due to improper access restrictions on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to access running configuration information about devices managed by the IND, including administrative credentials. **CVE ID : CVE-2019-1976**		
webex_teams					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-09-2019	9.3	A vulnerability in the Cisco Webex Teams client for Windows could allow an unauthenticated, remote attacker to execute arbitrary commands on an affected system. This vulnerability is due to improper restrictions on software logging features used by the application on Windows operating systems. An attacker could exploit this vulnerability by convincing a targeted user to visit a website designed to submit malicious input to the affected application. A successful exploit could allow the attacker to cause the application to modify files and execute arbitrary commands on the system with the privileges of the targeted user.	N/A	A-CIS-WEBE-230919/51

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		🟥	**CVE ID : CVE-2019-1939**		
identity_services_engine					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-09-2019	4.3	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability exists because the web-based management interface of the affected device does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2019-12644**	N/A	A-CIS-IDEN-230919/52
unified_contact_center_express					
Server-Side Request Forgery (SSRF)	04-09-2019	5	A vulnerability in Cisco Unified Contact Center Express (Unified CCX) could allow an unauthenticated, remote attacker to bypass access controls and conduct a server-side request forgery (SSRF) attack on a targeted system. The vulnerability is due to improper validation of user-supplied input on the	N/A	A-CIS-UNIF-230919/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected system. An attacker could exploit this vulnerability by sending the user of the web application a crafted request. If the request is processed, the attacker could access the system and perform unauthorized actions. **CVE ID : CVE-2019-12633**		
finesse					
Improper Input Validation	04-09-2019	5	A vulnerability in Cisco Finesse could allow an unauthenticated, remote attacker to bypass access controls and conduct a server-side request forgery (SSRF) attack on an affected system. The vulnerability exists because the affected system does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to access the system and perform unauthorized actions. **CVE ID : CVE-2019-12632**	N/A	A-CIS-FINE-230919/54
content_security_management_appliance					
Improper Authorizatio n	04-09-2019	4	A vulnerability in the authorization module of Cisco Content Security Management Appliance (SMA) Software could allow an authenticated, remote attacker to gain out-of-scope	N/A	A-CIS-CONT-230919/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to email. The vulnerability exists because the affected software does not correctly implement role permission controls. An attacker could exploit this vulnerability by using a custom role with specific permissions. A successful exploit could allow the attacker to access the spam quarantine of other users. **CVE ID : CVE-2019-12635**		
jabber					
Improper Input Validation	04-09-2019	7.2	A vulnerability in Cisco Jabber Client Framework (JCF) for Mac Software, installed as part of the Cisco Jabber for Mac client, could allow an authenticated, local attacker to execute arbitrary code on an affected device The vulnerability is due to improper file level permissions on an affected device when it is running Cisco JCF for Mac Software. An attacker could exploit this vulnerability by authenticating to the affected device and executing arbitrary code or potentially modifying certain configuration files. A successful exploit could allow the attacker to execute arbitrary code or modify certain configuration files on the device using the privileges of the installed	N/A	A-CIS-JABB-230919/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco JCF for Mac Software. **CVE ID : CVE-2019-12645**		
compact_arena_project					
compact_arena					
Out-of-bounds Write	09-09-2019	9	An issue was discovered in the compact_arena crate before 0.4.0 for Rust. Generativity is mishandled, leading to an out-of-bounds write or read. **CVE ID : CVE-2019-16139**	N/A	A-COM-COMP-230919/57
convertplug					
convertplus					
Improper Input Validation	03-09-2019	5	The ConvertPlus plugin before 3.4.5 for WordPress has an unintended account creation (with the none role) via a request for variants. **CVE ID : CVE-2019-15863**	N/A	A-CON-CONV-230919/58
couchbase					
couchbase_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-09-2019	4.3	An issue was discovered in Couchbase Server 5.1.2 and 5.5.0. The http server on port 8092 lacks an X-XSS protection header. **CVE ID : CVE-2019-11464**	N/A	A-COU-COUC-230919/59
Information Exposure Through Discrepancy	10-09-2019	5	An issue was discovered in Couchbase Server 5.5.x through 5.5.3 and 6.0.0. The Memcached "connections" stat block command emits a non-redacted username. The system information submitted to Couchbase as	N/A	A-COU-COUC-230919/60

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			part of a bug report included the usernames for all users currently logged into the system even if the log was redacted for privacy. This has been fixed (in 5.5.4 and 6.0.1) so that usernames are tagged properly in the logs and are hashed out when the logs are redacted. **CVE ID : CVE-2019-11465**		
Improper Authentication	10-09-2019	5	An issue was discovered in Couchbase Server 5.5.0 and 6.0.0. The Eventing debug endpoint mishandles authentication and audit. **CVE ID : CVE-2019-11466**	N/A	A-COU-COUC-230919/61
Uncontrolled Resource Consumption	10-09-2019	7.8	An issue was discovered in Couchbase Server 4.6.3 and 5.5.0. A JSON document to be stored with more than 3000 '\t' characters can crash the indexing system. **CVE ID : CVE-2019-11467**	N/A	A-COU-COUC-230919/62
Improper Control of Generation of Code ('Code Injection')	10-09-2019	7.5	Couchbase Server 5.1.1 generates insufficiently random numbers. The product hosts many network services by default. One of those services is an epmd service, which allows for node integration between Erlang instances. This service is protected by a single 16-character password. Unfortunately, this password is not generated securely due to an insufficient random seed, and can be reasonably	N/A	A-COU-COUC-230919/63

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			brute-forced by an attacker to execute code against a remote system. **CVE ID : CVE-2019-11495**		
Improper Authentication	10-09-2019	6.4	An issue was discovered in Couchbase Server 5.0.0. Editing bucket settings resets credentials, and leads to authorization without credentials. **CVE ID : CVE-2019-11496**	N/A	A-COU-COUC-230919/64
Improper Certificate Validation	10-09-2019	5	An issue was discovered in Couchbase Server 5.0.0. When creating a new remote cluster reference in Couchbase for XDCR, an invalid certificate is accepted. (The correct behavior is to validate the certificate against the remote cluster.) **CVE ID : CVE-2019-11497**	N/A	A-COU-COUC-230919/65
crelly_slider_project					
crelly_slider					
Unrestricted Upload of File with Dangerous Type	03-09-2019	6.5	The crelly-slider plugin before 1.3.5 for WordPress has arbitrary file upload via a PHP file inside a ZIP archive to wp_ajax_crellyslider_importSlider. **CVE ID : CVE-2019-15866**	N/A	A-CRE-CREL-230919/66
Cybozu					
garoon					
Improper Neutralization of Special Elements in	12-09-2019	3.5	DOM-based cross-site scripting vulnerability in Cybozu Garoon 4.6.0 to 4.10.2 allows remote	N/A	A-CYB-GARO-230919/67

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Output Used by a Downstream Component ('Injection')			authenticated attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE ID : CVE-2019-5975**		
Improper Input Validation	12-09-2019	4	Cybozu Garoon 4.0.0 to 4.10.2 allows an attacker with administrative rights to cause a denial of service condition via unspecified vectors. **CVE ID : CVE-2019-5976**	N/A	A-CYB-GARO-230919/68
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-09-2019	4	Mail header injection vulnerability in Cybozu Garoon 4.0.0 to 4.10.2 may allow a remote authenticated attackers to alter mail header via the application 'E-Mail'. **CVE ID : CVE-2019-5977**	N/A	A-CYB-GARO-230919/69
URL Redirection to Untrusted Site ('Open Redirect')	12-09-2019	5.8	Open redirect vulnerability in Cybozu Garoon 4.0.0 to 4.10.2 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via the application 'Scheduler'. **CVE ID : CVE-2019-5978**	N/A	A-CYB-GARO-230919/70
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-09-2019	6.5	SQL injection vulnerability in the Cybozu Garoon 4.0.0 to 4.10.3 allows remote authenticated attackers to execute arbitrary SQL commands via unspecified vectors. **CVE ID : CVE-2019-5991**	N/A	A-CYB-GARO-230919/71

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dell					
emc_unity_operating_environment					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-09-2019	4.3	Dell EMC Unity Operating Environment versions prior to 5.0.0.0.5.116, Dell EMC UnityVSA versions prior to 5.0.0.0.5.116 and Dell EMC VNXe3200 versions prior to 3.1.10.9946299 contain a reflected cross-site scripting vulnerability on the cas/logout page. A remote unauthenticated attacker could potentially exploit this vulnerability by tricking a victim application user to supply malicious HTML or Java Script code to Unisphere, which is then reflected back to the victim and executed by the web browser. **CVE ID : CVE-2019-3754**	https://www.dell.com/support/security/en-us/details/536796/DSA-2019-125-Dell-EMC-Unity-and-VNXe3200-Family-Reflected-Cross-Site-Scripting-Vulnerability	A-DEL-EMC_-230919/72
emc_unityvsa_operating_environment					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-09-2019	4.3	Dell EMC Unity Operating Environment versions prior to 5.0.0.0.5.116, Dell EMC UnityVSA versions prior to 5.0.0.0.5.116 and Dell EMC VNXe3200 versions prior to 3.1.10.9946299 contain a reflected cross-site scripting vulnerability on the cas/logout page. A remote unauthenticated attacker could potentially exploit this vulnerability by tricking a victim application user to supply malicious HTML or Java Script code to	https://www.dell.com/support/security/en-us/details/536796/DSA-2019-125-Dell-EMC-Unity-and-VNXe3200-Family-Reflected-Cross-Site-Scripting-Vulnerabilit	A-DEL-EMC_-230919/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Unisphere, which is then reflected back to the victim and executed by the web browser. **CVE ID : CVE-2019-3754**	y	
emc_enterprise_copy_data_management					
Improper Certificate Validation	03-09-2019	5.8	Dell EMC Enterprise Copy Data Management (eCDM) versions 1.0, 1.1, 2.0, 2.1, and 3.0 contain a certificate validation vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to carry out a man-in-the-middle attack by supplying a crafted certificate and intercepting the victim's traffic to view or modify a victim?s data in transit. **CVE ID : CVE-2019-3751**	N/A	A-DEL-EMC_-230919/74
rsa_identity_governance_and_lifecycle					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	3.5	The RSA Identity Governance and Lifecycle software and RSA Via Lifecycle and Governance products prior to 7.1.0 P08 contain a stored cross-site scripting vulnerability in the Access Request module. A remote authenticated malicious user could potentially exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the stored malicious code would gets	https://www.dell.com/support/security/en-us/details/DOC-106943/DSA-2019-134-RSA-Identity-Governance-and-Lifecycle-Product-Security-Update-for-Multiple-	A-DEL-RSA_-230919/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executed by the web browser in the context of the vulnerable web application. **CVE ID : CVE-2019-3761**	Vulnerabi	
Information Exposure	11-09-2019	2.1	The RSA Identity Governance and Lifecycle software and RSA Via Lifecycle and Governance products prior to 7.1.0 P08 contain an information exposure vulnerability. The Office 365 user password may get logged in a plain text format in the Office 365 connector debug log file. An authenticated malicious local user with access to the debug logs may obtain the exposed password to use in further attacks. **CVE ID : CVE-2019-3763**	https://www.dell.com/support/security/en-us/details/DOC-106943/DSA-2019-134-RSA-Identity-Governance-and-Lifecycle-Product-Security-Update-for-Multiple-Vulnerabi	A-DEL-RSA_-230919/76
Improper Control of Generation of Code ('Code Injection')	11-09-2019	5.5	The RSA Identity Governance and Lifecycle software and RSA Via Lifecycle and Governance products prior to 7.1.0 P08 contain a code injection vulnerability. A remote authenticated malicious user could potentially exploit this vulnerability to run custom Groovy scripts to gain limited access to view or modify information on the Workflow system. **CVE ID : CVE-2019-3759**	https://www.dell.com/support/security/en-us/details/DOC-106943/DSA-2019-134-RSA-Identity-Governance-and-Lifecycle-Product-Security-Update-for-Multiple-Vulnerabi	A-DEL-RSA_-230919/77

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-09-2019	6.5	The RSA Identity Governance and Lifecycle software and RSA Via Lifecycle and Governance products prior to 7.1.0 P08 contain a SQL Injection vulnerability in Workflow Architect. A remote authenticated malicious user could potentially exploit this vulnerability to execute SQL commands on the back-end database to gain unauthorized access to the data by supplying specially crafted input data to the affected application. **CVE ID : CVE-2019-3760**	https://www.dell.com/support/security/en-us/details/DOC-106943/DSA-2019-134-RSA-Identity-Governance-and-Lifecycle-Product-Security-Update-for-Multiple-Vulnerabi	A-DEL-RSA_-230919/78
rsa_via_lifecycle_and_governance					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	3.5	The RSA Identity Governance and Lifecycle software and RSA Via Lifecycle and Governance products prior to 7.1.0 P08 contain a stored cross-site scripting vulnerability in the Access Request module. A remote authenticated malicious user could potentially exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the stored malicious code would gets executed by the web browser in the context of the vulnerable web application. **CVE ID : CVE-2019-3761**	https://www.dell.com/support/security/en-us/details/DOC-106943/DSA-2019-134-RSA-Identity-Governance-and-Lifecycle-Product-Security-Update-for-Multiple-Vulnerabi	A-DEL-RSA_-230919/79

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	11-09-2019	2.1	The RSA Identity Governance and Lifecycle software and RSA Via Lifecycle and Governance products prior to 7.1.0 P08 contain an information exposure vulnerability. The Office 365 user password may get logged in a plain text format in the Office 365 connector debug log file. An authenticated malicious local user with access to the debug logs may obtain the exposed password to use in further attacks. **CVE ID : CVE-2019-3763**	https://www.dell.com/support/security/en-us/details/DOC-106943/DSA-2019-134-RSA-Identity-Governance-and-Lifecycle-Product-Security-Update-for-Multiple-Vulnerabi	A-DEL-RSA_-230919/80
Improper Control of Generation of Code ('Code Injection')	11-09-2019	5.5	The RSA Identity Governance and Lifecycle software and RSA Via Lifecycle and Governance products prior to 7.1.0 P08 contain a code injection vulnerability. A remote authenticated malicious user could potentially exploit this vulnerability to run custom Groovy scripts to gain limited access to view or modify information on the Workflow system. **CVE ID : CVE-2019-3759**	https://www.dell.com/support/security/en-us/details/DOC-106943/DSA-2019-134-RSA-Identity-Governance-and-Lifecycle-Product-Security-Update-for-Multiple-Vulnerabi	A-DEL-RSA_-230919/81
Improper Neutralization of Special Elements used in an	11-09-2019	6.5	The RSA Identity Governance and Lifecycle software and RSA Via Lifecycle and Governance products prior to 7.1.0 P08 contain a SQL	https://www.dell.com/support/security/en-us/details/D	A-DEL-RSA_-230919/82

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			Injection vulnerability in Workflow Architect. A remote authenticated malicious user could potentially exploit this vulnerability to execute SQL commands on the back-end database to gain unauthorized access to the data by supplying specially crafted input data to the affected application. **CVE ID : CVE-2019-3760**	OC-106943/DSA-2019-134-RSA-Identity-Governance-and-Lifecycle-Product-Security-Update-for-Multiple-Vulnerabi	
deltaww					
dcisoft					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	4.6	Delta DCISoft 1.21 has a User Mode Write AV starting at CommLib!CCommLib::SetSerializeData+0x0000000000000001b. **CVE ID : CVE-2019-16247**	N/A	A-DEL-DCIS-230919/83
tpeditor					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	11-09-2019	6.8	Delta Electronics TPEditor, Versions 1.94 and prior. Multiple heap-based buffer overflow vulnerabilities may be exploited by processing specially crafted project files, which may allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2019-13536**	N/A	A-DEL-TPED-230919/84
Improper Restriction of Operations within the	11-09-2019	6.8	Delta Electronics TPEditor, Versions 1.94 and prior. Multiple stack-based buffer overflow vulnerabilities may be exploited by processing	N/A	A-DEL-TPED-230919/85

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			specially crafted project files, which may allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2019-13540**		
Out-of-bounds Write	11-09-2019	6.8	Delta Electronics TPEditor, Versions 1.94 and prior. Multiple out-of-bounds write vulnerabilities may be exploited by processing specially crafted project files, which may allow remote code execution. **CVE ID : CVE-2019-13544**	N/A	A-DEL-TPED-230919/86
Digium					
asterisk					
NULL Pointer Dereference	09-09-2019	4	res_pjsip_t38 in Sangoma Asterisk 13.21-cert4, 15.7.3, and 16.5.0 allows an attacker to trigger a crash by sending a declined stream in a response to a T.38 re-invite initiated by Asterisk. **CVE ID : CVE-2019-15297**	N/A	A-DIG-ASTE-230919/87
Improper Input Validation	09-09-2019	5	main/translate.c in Sangoma Asterisk 13.28.0 and 16.5.0 allows a remote attacker to send a specific RTP packet during a call and cause a crash in a specific scenario. **CVE ID : CVE-2019-15639**	N/A	A-DIG-ASTE-230919/88
doccms					
doccms					
Improper Privilege Management	09-09-2019	7.5	upload_model() in /admini/controllers/system/managemodel.php in DocCms 2016.5.17 allow remote	N/A	A-DOC-DOCC-230919/89

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute arbitrary PHP code through module management files, as demonstrated by a .php file in a ZIP archive. **CVE ID : CVE-2019-16192**		
Easy!appointments_project					
Easy!appointments					
Information Exposure	11-09-2019	5	Easy!Appointments 1.3.2 plugin for WordPress allows Sensitive Information Disclosure (Username and Password Hash). **CVE ID : CVE-2019-14936**	N/A	A-EAS-EASY-230919/90
Eclipse					
omr					
Improper Control of Generation of Code ('Code Injection')	12-09-2019	4.6	Prior to 0.1, AIX builds of Eclipse OMR contain unused RPATHs which may facilitate code injection and privilege elevation by local users. **CVE ID : CVE-2019-11773**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=549191	A-ECL-OMR-230919/91
paho_java_client					
Improper Input Validation	11-09-2019	5	In the Eclipse Paho Java client library version 1.2.0, when connecting to an MQTT server using TLS and setting a host name verifier, the result of that verification is not checked. This could allow one MQTT server to impersonate another and provide the client library with incorrect information. **CVE ID : CVE-2019-11777**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=549934	A-ECL-PAHO-230919/92
egain					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
chat					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-09-2019	4.3	eGain Chat 15.0.3 allows HTML Injection. **CVE ID : CVE-2019-13975**	N/A	A-EGA-CHAT-230919/93
Unrestricted Upload of File with Dangerous Type	04-09-2019	7.5	eGain Chat 15.0.3 allows unrestricted file upload. **CVE ID : CVE-2019-13976**	N/A	A-EGA-CHAT-230919/94
ENG					
knowage					
Improper Access Control	05-09-2019	5	In Knowage through 6.1.1, an unauthenticated user can bypass access controls and access the entire application. **CVE ID : CVE-2019-13188**	N/A	A-ENG-KNOW-230919/95
Improper Authentication	05-09-2019	5	In Knowage through 6.1.1, the sign up page does not invalidate a valid CAPTCHA token. This allows for CAPTCHA bypass in the signup page. **CVE ID : CVE-2019-13190**	N/A	A-ENG-KNOW-230919/96
epignosishq					
efront_lms					
Deserialization of Untrusted Data	05-09-2019	6.5	A code execution vulnerability exists in Epignosis eFront LMS v5.2.12. A specially crafted web request can cause unsafe deserialization potentially resulting in PHP code being	N/A	A-EPI-EFRO-230919/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executed. An attacker can send a crafted web parameter to trigger this vulnerability. **CVE ID : CVE-2019-5069**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-09-2019	6.4	An exploitable SQL injection vulnerability exists in the unauthenticated portion of eFront LMS, versions v5.2.12 and earlier. Specially crafted web request to login page can cause SQL injections, resulting in data compromise. An attacker can use a browser to trigger these vulnerabilities, and no special tools are required. **CVE ID : CVE-2019-5070**	N/A	A-EPI-EFRO-230919/98
espressif					
arduino-esp32					
Improper Input Validation	04-09-2019	3.3	The EAP peer implementation in Espressif ESP-IDF 2.0.0 through 4.0.0 and ESP8266_NONOS_SDK 2.2.0 through 3.1.0 processes EAP Success messages before any EAP method completion or failure, which allows attackers in radio range to cause a denial of service (crash) via a crafted message. **CVE ID : CVE-2019-12586**	N/A	A-ESP-ARDU-230919/99
esp-idf					
Improper Input Validation	04-09-2019	3.3	The EAP peer implementation in Espressif ESP-IDF 2.0.0 through 4.0.0 and ESP8266_NONOS_SDK 2.2.0 through 3.1.0 processes	N/A	A-ESP-ESP--230919/100

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EAP Success messages before any EAP method completion or failure, which allows attackers in radio range to cause a denial of service (crash) via a crafted message. **CVE ID : CVE-2019-12586**		
Improper Input Validation	04-09-2019	4.8	The EAP peer implementation in Espressif ESP-IDF 2.0.0 through 4.0.0 and ESP8266_NONOS_SDK 2.2.0 through 3.1.0 allows the installation of a zero Pairwise Master Key (PMK) after the completion of any EAP authentication method, which allows attackers in radio range to replay, decrypt, or spoof frames via a rogue access point. **CVE ID : CVE-2019-12587**	N/A	A-ESP-ESP--230919/101
esp8266_nonos_sdk					
Improper Input Validation	04-09-2019	3.3	The EAP peer implementation in Espressif ESP-IDF 2.0.0 through 4.0.0 and ESP8266_NONOS_SDK 2.2.0 through 3.1.0 processes EAP Success messages before any EAP method completion or failure, which allows attackers in radio range to cause a denial of service (crash) via a crafted message. **CVE ID : CVE-2019-12586**	N/A	A-ESP-ESP8-230919/102
Improper Input Validation	04-09-2019	4.8	The EAP peer implementation in Espressif ESP-IDF 2.0.0 through 4.0.0 and ESP8266_NONOS_SDK 2.2.0 through 3.1.0 allows the	N/A	A-ESP-ESP8-230919/103

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			installation of a zero Pairwise Master Key (PMK) after the completion of any EAP authentication method, which allows attackers in radio range to replay, decrypt, or spoof frames via a rogue access point. **CVE ID : CVE-2019-12587**		
Improper Input Validation	04-09-2019	3.3	The client 802.11 mac implementation in Espressif ESP8266_NONOS_SDK 2.2.0 through 3.1.0 does not validate correctly the RSN AuthKey suite list count in beacon frames, probe responses, and association responses, which allows attackers in radio range to cause a denial of service (crash) via a crafted message. **CVE ID : CVE-2019-12588**	N/A	A-ESP-ESP8-230919/104
arduino_esp8266					
Improper Input Validation	04-09-2019	3.3	The client 802.11 mac implementation in Espressif ESP8266_NONOS_SDK 2.2.0 through 3.1.0 does not validate correctly the RSN AuthKey suite list count in beacon frames, probe responses, and association responses, which allows attackers in radio range to cause a denial of service (crash) via a crafted message. **CVE ID : CVE-2019-12588**	N/A	A-ESP-ARDU-230919/105
Esri					
arcgis_enterprise					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	3.5	In ArcGIS Enterprise 10.6.1, a crafted IFRAME element can be used to trigger a Cross Frame Scripting (XFS) attack through the EDIT MY PROFILE feature. **CVE ID : CVE-2019-16193**	N/A	A-ESR-ARCG-230919/106
Estrongs					
es_file_explorer_file_manager					
Improper Access Control	05-09-2019	5	The master-password feature in the ES File Explorer File Manager application 4.2.0.1.3 for Android can be bypassed via a com.estrongs.android.pop.ftp.ESFtpShortcut intent, leading to remote FTP access to the entirety of local storage. **CVE ID : CVE-2019-11380**	N/A	A-EST-ES_F-230919/107
Exim					
exim					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-09-2019	10	Exim before 4.92.2 allows remote attackers to execute arbitrary code as root via a trailing backslash. **CVE ID : CVE-2019-15846**	N/A	A-EXI-EXIM-230919/108
ezautomation					
ez_touch_editor					
Improper Restriction of Operations within the	04-09-2019	6.8	An attacker could use a specially crafted project file to overflow the buffer and execute code under the privileges of the EZ Touch	N/A	A-EZA-EZ_T-230919/109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Editor Versions 2.1.0 and prior. **CVE ID : CVE-2019-13518**		
ez_plc_editor					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-09-2019	6.8	An attacker could use a specially crafted project file to corrupt the memory and execute code under the privileges of the EZ PLC Editor Versions 1.8.41 and prior. **CVE ID : CVE-2019-13522**	N/A	A-EZA-EZ_P-230919/110
F5					
container_ingress_service					
Information Exposure Through Log Files	04-09-2019	1.9	On version 1.9.0, If DEBUG logging is enable, F5 Container Ingress Service (CIS) for Kubernetes and Red Hat OpenShift (k8s-bigip-ctlr) log files may contain BIG-IP secrets such as SSL Private Keys and Private key Passphrases as provided as inputs by an AS3 Declaration. **CVE ID : CVE-2019-6648**	N/A	A-F5-CONT-230919/111
big-ip_access_policy_manager					
Improper Input Validation	04-09-2019	5	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file.	N/A	A-F5-BIG--230919/112

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6643		
Improper Authorization	04-09-2019	6.8	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible. **CVE ID : CVE-2019-6644**	N/A	A-F5-BIG--230919/113
Improper Input Validation	04-09-2019	5	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken. **CVE ID : CVE-2019-6645**	N/A	A-F5-BIG--230919/114
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges. **CVE ID : CVE-2019-6646**	N/A	A-F5-BIG--230919/115
Uncontrolled Resource Consumption	04-09-2019	4.3	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for	N/A	A-F5-BIG--230919/116

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system. **CVE ID : CVE-2019-6647**		
big-ip_advanced_firewall_manager					
Improper Input Validation	04-09-2019	5	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file. **CVE ID : CVE-2019-6643**	N/A	A-F5-BIG--230919/117
Improper Authorization	04-09-2019	6.8	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible. **CVE ID : CVE-2019-6644**	N/A	A-F5-BIG--230919/118
Improper Input Validation	04-09-2019	5	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual	N/A	A-F5-BIG--230919/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken. **CVE ID : CVE-2019-6645**		
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges. **CVE ID : CVE-2019-6646**	N/A	A-F5-BIG--230919/120
Uncontrolled Resource Consumption	04-09-2019	4.3	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system. **CVE ID : CVE-2019-6647**	N/A	A-F5-BIG--230919/121
big-ip_analytics					
Improper Input Validation	04-09-2019	5	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may	N/A	A-F5-BIG--230919/122

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be able to cause the TMM process to produce a core file. **CVE ID : CVE-2019-6643**		
Improper Authorization	04-09-2019	6.8	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible. **CVE ID : CVE-2019-6644**	N/A	A-F5-BIG--230919/123
Improper Input Validation	04-09-2019	5	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken. **CVE ID : CVE-2019-6645**	N/A	A-F5-BIG--230919/124
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges. **CVE ID : CVE-2019-6646**	N/A	A-F5-BIG--230919/125
Uncontrolled Resource	04-09-2019	4.3	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2,	N/A	A-F5-BIG--

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system. **CVE ID : CVE-2019-6647**		230919/126
big-ip_application_acceleration_manager					
Improper Input Validation	04-09-2019	5	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file. **CVE ID : CVE-2019-6643**	N/A	A-F5-BIG--230919/127
Improper Authorization	04-09-2019	6.8	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible. **CVE ID : CVE-2019-6644**	N/A	A-F5-BIG--230919/128
Improper	04-09-2019	5	On BIG-IP 14.0.0-14.1.0.5,	N/A	A-F5-BIG--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken. **CVE ID : CVE-2019-6645**		230919/129
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges. **CVE ID : CVE-2019-6646**	N/A	A-F5-BIG--230919/130
Uncontrolled Resource Consumption	04-09-2019	4.3	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system. **CVE ID : CVE-2019-6647**	N/A	A-F5-BIG--230919/131
big-ip_application_security_manager					
Improper Input Validation	04-09-2019	5	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6	N/A	A-F5-BIG--230919/132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file. **CVE ID : CVE-2019-6643**		
Improper Authorization	04-09-2019	6.8	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible. **CVE ID : CVE-2019-6644**	N/A	A-F5-BIG--230919/133
Improper Input Validation	04-09-2019	5	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken. **CVE ID : CVE-2019-6645**	N/A	A-F5-BIG--230919/134
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges.	N/A	A-F5-BIG--230919/135

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6646		
Uncontrolled Resource Consumption	04-09-2019	4.3	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system. **CVE ID : CVE-2019-6647**	N/A	A-F5-BIG--230919/136
big-ip_domain_name_system					
Improper Input Validation	04-09-2019	5	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file. **CVE ID : CVE-2019-6643**	N/A	A-F5-BIG--230919/137
Improper Authorizatio n	04-09-2019	6.8	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is	N/A	A-F5-BIG--230919/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible. **CVE ID : CVE-2019-6644**		
Improper Input Validation	04-09-2019	5	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken. **CVE ID : CVE-2019-6645**	N/A	A-F5-BIG--230919/139
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges. **CVE ID : CVE-2019-6646**	N/A	A-F5-BIG--230919/140
Uncontrolled Resource Consumption	04-09-2019	4.3	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system. **CVE ID : CVE-2019-6647**	N/A	A-F5-BIG--230919/141
big-ip_edge_gateway					
Improper	04-09-2019	5	On versions 14.1.0-14.1.0.5,	N/A	A-F5-BIG--

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file. **CVE ID : CVE-2019-6643**		230919/142
Improper Authorization	04-09-2019	6.8	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible. **CVE ID : CVE-2019-6644**	N/A	A-F5-BIG--230919/143
Improper Input Validation	04-09-2019	5	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken. **CVE ID : CVE-2019-6645**	N/A	A-F5-BIG--230919/144
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest	N/A	A-F5-BIG--230919/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges may be able to escalate their privileges and run commands with admin privileges. **CVE ID : CVE-2019-6646**		
Uncontrolled Resource Consumption	04-09-2019	4.3	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system. **CVE ID : CVE-2019-6647**	N/A	A-F5-BIG--230919/146
big-ip_fraud_protection_service					
Improper Input Validation	04-09-2019	5	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file. **CVE ID : CVE-2019-6643**	N/A	A-F5-BIG--230919/147
Improper Authorizatio n	04-09-2019	6.8	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when	N/A	A-F5-BIG--230919/148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible. **CVE ID : CVE-2019-6644**		
Improper Input Validation	04-09-2019	5	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken. **CVE ID : CVE-2019-6645**	N/A	A-F5-BIG--230919/149
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges. **CVE ID : CVE-2019-6646**	N/A	A-F5-BIG--230919/150
Uncontrolled Resource Consumption	04-09-2019	4.3	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system.	N/A	A-F5-BIG--230919/151

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6647		
big-ip_global_traffic_manager					
Improper Input Validation	04-09-2019	5	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file. **CVE ID : CVE-2019-6643**	N/A	A-F5-BIG--230919/152
Improper Authorization	04-09-2019	6.8	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible. **CVE ID : CVE-2019-6644**	N/A	A-F5-BIG--230919/153
Improper Input Validation	04-09-2019	5	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken. **CVE ID : CVE-2019-6645**	N/A	A-F5-BIG--230919/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges. **CVE ID : CVE-2019-6646**	N/A	A-F5-BIG--230919/155
Uncontrolled Resource Consumption	04-09-2019	4.3	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system. **CVE ID : CVE-2019-6647**	N/A	A-F5-BIG--230919/156
big-ip_link_controller					
Improper Input Validation	04-09-2019	5	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file. **CVE ID : CVE-2019-6643**	N/A	A-F5-BIG--230919/157
Improper Authorization	04-09-2019	6.8	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2,	N/A	A-F5-BIG--230919/158

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible. **CVE ID : CVE-2019-6644**		
Improper Input Validation	04-09-2019	5	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken. **CVE ID : CVE-2019-6645**	N/A	A-F5-BIG--230919/159
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges. **CVE ID : CVE-2019-6646**	N/A	A-F5-BIG--230919/160
Uncontrolled Resource Consumption	04-09-2019	4.3	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management	N/A	A-F5-BIG--230919/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface could eventually deplete memory on the system. **CVE ID : CVE-2019-6647**		
big-ip_local_traffic_manager					
Improper Input Validation	04-09-2019	5	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file. **CVE ID : CVE-2019-6643**	N/A	A-F5-BIG--230919/162
Improper Authorization	04-09-2019	6.8	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible. **CVE ID : CVE-2019-6644**	N/A	A-F5-BIG--230919/163
Improper Input Validation	04-09-2019	5	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the	N/A	A-F5-BIG--230919/164

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configured HA action to be taken. **CVE ID : CVE-2019-6645**		
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges. **CVE ID : CVE-2019-6646**	N/A	A-F5-BIG--230919/165
Uncontrolled Resource Consumption	04-09-2019	4.3	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system. **CVE ID : CVE-2019-6647**	N/A	A-F5-BIG--230919/166
big-ip_policy_enforcement_manager					
Improper Input Validation	04-09-2019	5	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file. **CVE ID : CVE-2019-6643**	N/A	A-F5-BIG--230919/167

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authorizatio n	04-09-2019	6.8	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible. **CVE ID : CVE-2019-6644**	N/A	A-F5-BIG--230919/168
Improper Input Validation	04-09-2019	5	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken. **CVE ID : CVE-2019-6645**	N/A	A-F5-BIG--230919/169
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges. **CVE ID : CVE-2019-6646**	N/A	A-F5-BIG--230919/170
Uncontrolled Resource Consumption	04-09-2019	4.3	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD	N/A	A-F5-BIG--230919/171

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system. **CVE ID : CVE-2019-6647**		
big-ip_webaccelerator					
Improper Input Validation	04-09-2019	5	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file. **CVE ID : CVE-2019-6643**	N/A	A-F5-BIG--230919/172
Improper Authorization	04-09-2019	6.8	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible. **CVE ID : CVE-2019-6644**	N/A	A-F5-BIG--230919/173
Improper Input Validation	04-09-2019	5	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active	N/A	A-F5-BIG--230919/174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken. **CVE ID : CVE-2019-6645**		
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges. **CVE ID : CVE-2019-6646**	N/A	A-F5-BIG--230919/175
Uncontrolled Resource Consumption	04-09-2019	4.3	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system. **CVE ID : CVE-2019-6647**	N/A	A-F5-BIG--230919/176
enterprise_manager					
N/A	04-09-2019	6.5	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges. **CVE ID : CVE-2019-6646**	N/A	A-F5-ENTE-230919/177

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Facebook					
hhvm					
Out-of-bounds Read	06-09-2019	7.5	Insufficient boundary checks when processing the JPEG APP12 block marker in the GD extension could allow access to out-of-bounds memory via a maliciously constructed invalid JPEG input. This issue affects HHVM versions prior to 3.30.9, all versions between 4.0.0 and 4.8.3, all versions between 4.9.0 and 4.15.2, and versions 4.16.0 to 4.16.3, 4.17.0 to 4.17.2, 4.18.0 to 4.18.1, 4.19.0, 4.20.0 to 4.20.1. **CVE ID : CVE-2019-11925**	https://www.facebook.com/security/advisories/cve-2019-11925	A-FAC-HHVM-230919/178
Out-of-bounds Read	06-09-2019	7.5	Insufficient boundary checks when processing M_SOFx markers from JPEG headers in the GD extension could allow access to out-of-bounds memory via a maliciously constructed invalid JPEG input. This issue affects HHVM versions prior to 3.30.9, all versions between 4.0.0 and 4.8.3, all versions between 4.9.0 and 4.15.2, and versions 4.16.0 to 4.16.3, 4.17.0 to 4.17.2, 4.18.0 to 4.18.1, 4.19.0, 4.20.0 to 4.20.1. **CVE ID : CVE-2019-11926**	https://www.facebook.com/security/advisories/cve-2019-11926	A-FAC-HHVM-230919/179
Ffmpeg					
ffmpeg					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-09-2019	6.8	FFmpeg through 4.2 has a "Conditional jump or move depends on uninitialised value" issue in h2645_parse because alloc_rbsp_buffer in libavcodec/h2645_parse.c mishandles rbsp_buffer. **CVE ID : CVE-2019-15942**	N/A	A-FFM-FFMP-230919/180
Freedesktop					
systemd					
Improper Access Control	04-09-2019	2.1	In systemd 240, bus_open_system_watch_bind_with_description in shared/bus-util.c (as used by systemd-resolved to connect to the system D-Bus instance), calls sd_bus_set_trusted, which disables access controls for incoming D-Bus messages. An unprivileged user can exploit this by executing D-Bus methods that should be restricted to privileged users, in order to change the system's DNS resolver settings. **CVE ID : CVE-2019-15718**	N/A	A-FRE-SYST-230919/181
fusionpbx					
fusionpbx					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-09-2019	9	FusionPBX 4.4.8 allows an attacker to execute arbitrary system commands by submitting a malicious command to the service_edit.php file (which will insert the malicious command into the database). To trigger the command, one	N/A	A-FUS-FUSI-230919/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needs to call the services.php file via a GET request with the service id followed by the parameter a=start to execute the stored command. **CVE ID : CVE-2019-15029**		
generator-rs_project					
generator-rs					
Improper Input Validation	09-09-2019	7.8	An issue was discovered in the generator crate before 0.6.18 for Rust. Uninitialized memory is used by Scope, done, and yield_ during API calls. **CVE ID : CVE-2019-16144**	N/A	A-GEN-GENE-230919/183
getgophish					
gophish					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-09-2019	3.5	Gophish through 0.8.0 allows XSS via a username. **CVE ID : CVE-2019-16146**	N/A	A-GET-GOPH-230919/184
getgrav					
grav_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-09-2019	4.3	Grav through 1.6.15 allows (Stored) Cross-Site Scripting due to JavaScript execution in SVG images. **CVE ID : CVE-2019-16126**	N/A	A-GET-GRAV-230919/185
Gitlab					
gitlab					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	09-09-2019	7.5	An issue was discovered in GitLab Community and Enterprise Edition 9.x, 10.x, and 11.x before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control. Access to the internal wiki is permitted when an external wiki service is enabled. **CVE ID : CVE-2019-6960**	https://gitlab.com/gitlab-org/gitlab-ce/issues/54357	A-GIT-GITL-230919/186
Incorrect Authorization	09-09-2019	4.3	An issue was discovered in GitLab Community and Enterprise Edition 8.x (starting in 8.9), 9.x, 10.x, and 11.x before 11.5.9, 11.6.x before 11.6.7, and 11.7.x before 11.7.2. It has Incorrect Access Control. Guest users are able to add reaction emojis on comments to which they have no visibility. **CVE ID : CVE-2019-7176**	https://gitlab.com/gitlab-org/gitlab-ce/issues/51332	A-GIT-GITL-230919/187
Information Exposure	09-09-2019	4	An issue was discovered in GitLab Community and Enterprise Edition 8.x, 9.x, 10.x, and 11.x before 11.8.9, 11.9.x before 11.9.10, and 11.10.x before 11.10.2. It allows Information Disclosure. Non-member users who subscribe to notifications of an internal project with issue and repository restrictions will receive emails about restricted events. **CVE ID : CVE-2019-11544**	https://gitlab.com/gitlab-org/gitlab-ce/issues/58372	A-GIT-GITL-230919/188
Information	09-09-2019	4	An issue was discovered in	https://gitla	A-GIT-GITL-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			GitLab Community Edition 11.9.x before 11.9.10 and 11.10.x before 11.10.2. It allows Information Disclosure. When an issue is moved to a private project, the private project namespace is leaked to unauthorized users with access to the original issue. **CVE ID : CVE-2019-11545**	b.com/gitlab-org/gitlab-ce/issues/58939	230919/189
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-09-2019	3.5	An issue was discovered in GitLab Community and Enterprise Edition before 11.8.9, 11.9.x before 11.9.10, and 11.10.x before 11.10.2. It has a Race Condition which could allow users to approve a merge request multiple times and potentially reach the approval count required to merge. **CVE ID : CVE-2019-11546**	https://gitlab.com/gitlab-org/gitlab-ee/issues/10357	A-GIT-GITL-230919/190
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-09-2019	4.3	An issue was discovered in GitLab Community and Enterprise Edition before 11.8.9, 11.9.x before 11.9.10, and 11.10.x before 11.10.2. It has Improper Encoding or Escaping of Output. The branch name on new merge request notification emails isn't escaped, which could potentially lead to XSS issues. **CVE ID : CVE-2019-11547**	https://gitlab.com/gitlab-org/gitlab-ee/issues/11515	A-GIT-GITL-230919/191
Improper Neutralization of Input During Web	09-09-2019	3.5	An issue was discovered in GitLab Community and Enterprise Edition before 11.8.9. It has Incorrect Access	https://gitlab.com/gitlab-org/gitlab-ce/issues/5	A-GIT-GITL-230919/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			Control. Unprivileged members of a project are able to post comments on confidential issues through an authorization issue in the note endpoint. **CVE ID : CVE-2019-11548**	8505	
Information Exposure	09-09-2019	4	An issue was discovered in GitLab Community and Enterprise Edition 9.x, 10.x, and 11.x before 11.8.9, 11.9.x before 11.9.10, and 11.10.x before 11.10.2. Gitaly has allows an information disclosure issue where HTTP/GIT credentials are included in logs on connection errors. **CVE ID : CVE-2019-11549**	https://gitlab.com/gitlab-org/gitlab-ce/issues/57779	A-GIT-GITL-230919/193
Information Exposure	09-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 11.8.x before 11.8.10, 11.9.x before 11.9.11, and 11.10.x before 11.10.3. It allows Information Disclosure. A small number of GitLab API endpoints would disclose project information when using a read_user scoped token. **CVE ID : CVE-2019-11605**	https://about.gitlab.com/2019/04/30/security-release-gitlab-11-dot-10-dot-3-released/	A-GIT-GITL-230919/194
Improper Authentication	09-09-2019	6.5	An authentication issue was discovered in GitLab that allowed a bypass of email verification. This was addressed in GitLab 12.1.2 and 12.0.4. **CVE ID : CVE-2019-5473**	N/A	A-GIT-GITL-230919/195

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	09-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows Information Disclosure (issue 1 of 6). An authorization issue allows the contributed project information of a private profile to be viewed. **CVE ID : CVE-2019-6782**	https://gitlab.com/gitlab-org/gitlab-ce/issues/52677	A-GIT-GITL-230919/196
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-09-2019	6.5	An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. GitLab Pages contains a directory traversal vulnerability that could lead to remote command execution. **CVE ID : CVE-2019-6783**	https://gitlab.com/gitlab-org/gitlab-ce/issues/55827	A-GIT-GITL-230919/197
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-09-2019	4.3	An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows XSS (issue 1 of 2). Markdown fields contain a lack of input validation and output encoding when processing KaTeX that results in a persistent XSS. **CVE ID : CVE-2019-6784**	https://gitlab.com/gitlab-org/gitlab-ce/issues/54416	A-GIT-GITL-230919/198
Improper Input Validation	09-09-2019	4	An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6,	https://gitlab.com/gitlab-org/gitlab-ce/issues/5	A-GIT-GITL-230919/199

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 11.7.x before 11.7.1. It allows Denial of Service. Inputting an overly long string into a Markdown field could cause a denial of service. **CVE ID : CVE-2019-6785**	2212	
Improper Input Validation	09-09-2019	4	An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control (issue 1 of 3). The contents of an LFS object can be accessed by an unauthorized user, if the file size and OID are known. **CVE ID : CVE-2019-6786**	https://gitlab.com/gitlab-org/gitlab-workhorse/issues/197	A-GIT-GITL-230919/200
Information Exposure	09-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows Information Disclosure (issue 3 of 6). For installations using GitHub or Bitbucket OAuth integrations, it is possible to use a covert redirect to obtain the user OAuth token for those services. **CVE ID : CVE-2019-6788**	https://gitlab.com/gitlab-org/gitlab-ce/issues/56663	A-GIT-GITL-230919/201
Information Exposure	09-09-2019	4	An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows Information	https://gitlab.com/gitlab-org/gitlab-ce/issues/44558	A-GIT-GITL-230919/202

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure (issue 4 of 6). In some cases, users without project permissions will receive emails after a project move. For private projects, this will disclose the new project namespace to an unauthorized user. **CVE ID : CVE-2019-6789**		
Improper Preservation of Permissions	09-09-2019	4	An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control (issue 3 of 3). When a project with visibility more permissive than the target group is imported, it will retain its prior visibility. **CVE ID : CVE-2019-6791**	https://about.gitlab.com/2019/01/31/security-release-gitlab-11-dot-7-dot-3-released/	A-GIT-GITL-230919/203
Information Exposure	09-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows Path Disclosure. When an error is encountered on project import, the error message will display instance internal information. **CVE ID : CVE-2019-6792**	https://gitlab.com/gitlab-org/gitlab-ce/issues/54867	A-GIT-GITL-230919/204
Server-Side Request Forgery (SSRF)	09-09-2019	6.8	An issue was discovered in GitLab Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. The Jira integration feature is vulnerable to an unauthenticated blind SSRF	https://gitlab.com/gitlab-org/gitlab-ce/issues/50748	A-GIT-GITL-230919/205

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue. **CVE ID : CVE-2019-6793**		
Information Exposure	09-09-2019	4	An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows Information Disclosure (issue 5 of 6). A project guest user can view the last commit status of the default branch. **CVE ID : CVE-2019-6794**	https://gitlab.com/gitlab-org/gitlab-ce/issues/54353	A-GIT-GITL-230919/206
Improper Input Validation	09-09-2019	5.8	An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Insufficient Visual Distinction of Homoglyphs Presented to a User. IDN homographs and RTLO characters are rendered to unicode, which could be used for social engineering. **CVE ID : CVE-2019-6795**	https://gitlab.com/gitlab-org/gitlab-ce/issues/29365	A-GIT-GITL-230919/207
Improper Preservation of Permissions	09-09-2019	4	An issue was discovered in GitLab Community and Enterprise Edition 8.x, 9.x, 10.x, and 11.x before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control. Users are able to comment on locked project issues. **CVE ID : CVE-2019-6995**	https://gitlab.com/gitlab-org/gitlab-ce/issues/55537	A-GIT-GITL-230919/208
Information Exposure	09-09-2019	4	An issue was discovered in GitLab Enterprise Edition 10.x (starting in 10.6) and	https://gitlab.com/gitlab-org/gitlab-	A-GIT-GITL-230919/209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.x before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control. The merge request approvers section has an access control issue that permits project maintainers to view membership of private groups. **CVE ID : CVE-2019-6996**	ee/issues/8187	
Information Exposure	09-09-2019	4	An issue was discovered in GitLab Community and Enterprise Edition 10.x (starting in 10.7) and 11.x before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control. System notes contain an access control issue that permits a guest user to view merge request titles. **CVE ID : CVE-2019-6997**	https://gitlab.com/gitlab-org/gitlab-ce/issues/53858	A-GIT-GITL-230919/210
glyphandcog					
xpdfreader					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-09-2019	6.8	In Xpdf 4.01.01, a stack-based buffer under-read could be triggered in IdentityFunction::transform in Function.cc, used by GfxAxialShading::getColor. It can, for example, be triggered by sending a crafted PDF document to the pdftoppm tool. It allows an attacker to use a crafted PDF file to cause Denial of Service or possibly unspecified other impact.	N/A	A-GLY-XPDF-230919/211

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16115		
Improper Input Validation	03-09-2019	4.3	Xpdf 2.00 allows a SIGSEGV in XRef::constructXRef in XRef.cc. NOTE: 2.00 is a version from November 2002. **CVE ID : CVE-2019-15860**	N/A	A-GLY-XPDF-230919/212
Uncontrolled Resource Consumption	06-09-2019	4.3	Xpdf 3.04 has a SIGSEGV in XRef::fetch in XRef.cc after many recursive calls to Catalog::countPageTree in Catalog.cc. **CVE ID : CVE-2019-16088**	N/A	A-GLY-XPDF-230919/213
GNU					
gcc					
Insufficient Entropy	02-09-2019	5	The POWER9 backend in GNU Compiler Collection (GCC) before version 10 could optimize multiple calls of the __builtin_darn intrinsic into a single call, thus reducing the entropy of the random number generator. This occurred because a volatile operation was not specified. For example, within a single execution of a program, the output of every __builtin_darn() call may be the same. **CVE ID : CVE-2019-15847**	N/A	A-GNU-GCC-230919/214
cflow					
Use After Free	09-09-2019	4.3	GNU cflow through 1.6 has a use-after-free in the reference function in parser.c. **CVE ID : CVE-2019-16165**	N/A	A-GNU-CFLO-230919/215

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	09-09-2019	4.3	GNU cflow through 1.6 has a heap-based buffer over-read in the nexttoken function in parser.c. **CVE ID : CVE-2019-16166**	N/A	A-GNU-CFLO-230919/216
grafana					
grafana					
Improper Access Control	03-09-2019	5	In Grafana 2.x through 6.x before 6.3.4, parts of the HTTP API allow unauthenticated use. This makes it possible to run a denial of service attack against the server running Grafana. **CVE ID : CVE-2019-15043**	N/A	A-GRA-GRAF-230919/217
hgw168cc					
yii-cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-09-2019	4.3	YII2-CMS v1.0 has XSS in protected\core\modules\home\models\Contact.php via a name field to /contact.html. **CVE ID : CVE-2019-16130**	N/A	A-HGW-YII--230919/218
humanica					
humatrix					
Incorrect Default Permissions	10-09-2019	5	The Recruitment module in Humanica Humatrix 7 1.0.0.203 and 1.0.0.681 allows an unauthenticated attacker to change the password of any user via the recruitment_online/personalData/act_acounttab.cfm txtNewUserName and hdNP	N/A	A-HUM-HUMA-230919/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fields. **CVE ID : CVE-2019-16106**		
IBM					
jazz_for_service_management					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-09-2019	4.3	IBM Jazz for Service Management 1.1.3 is vulnerable to HTTP header injection, caused by incorrect trust in the HTTP Host header during caching. By sending a specially crafted HTTP GET request, a remote attacker could exploit this vulnerability to inject arbitrary HTTP headers, which will allow the attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-force ID: 158976. **CVE ID : CVE-2019-4186**	https://supportcontent.ibm.com/support/pages/node/1071966	A-IBM-JAZZ-230919/220
intelligent_operations_center					
N/A	05-09-2019	5	IBM Intelligent Operations Center V5.1.0 - V5.2.0, IBM Intelligent Operations Center for Emergency Management V5.1.0 - V5.1.0.6, and IBM Water Operations for Waternamics V5.1.0 - V5.2.1.1 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 161201.	N/A	A-IBM-INTE-230919/221

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-4321		
intelligent_operations_center_for_emergency_management					
N/A	05-09-2019	5	IBM Intelligent Operations Center V5.1.0 - V5.2.0, IBM Intelligent Operations Center for Emergency Management V5.1.0 - V5.1.0.6, and IBM Water Operations for Waternamics V5.1.0 - V5.2.1.1 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 161201. **CVE ID : CVE-2019-4321**	N/A	A-IBM-INTE-230919/222
water_operations_for_waternamics					
N/A	05-09-2019	5	IBM Intelligent Operations Center V5.1.0 - V5.2.0, IBM Intelligent Operations Center for Emergency Management V5.1.0 - V5.1.0.6, and IBM Water Operations for Waternamics V5.1.0 - V5.2.1.1 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 161201. **CVE ID : CVE-2019-4321**	N/A	A-IBM-WATE-230919/223
business_automation_workflow					
Improper Neutralization of Input During Web Page	05-09-2019	3.5	IBM Business Automation Workflow V18.0.0.0 through V18.0.0.2 and IBM Business Process Manager V8.6.0.0 through V8.6.0.0 Cumulative	https://www.ibm.com/support/docview.wss?uid=ibm1088	A-IBM-BUSI-230919/224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Fix 2018.03, V8.5.7.0 through V8.5.7.0 Cumulative Fix 2017.06, and V8.5.6.0 through V8.5.6.0 CF2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158415. **CVE ID : CVE-2019-4149**	5104	
business_process_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-09-2019	3.5	IBM Business Automation Workflow V18.0.0.0 through V18.0.0.2 and IBM Business Process Manager V8.6.0.0 through V8.6.0.0 Cumulative Fix 2018.03, V8.5.7.0 through V8.5.7.0 Cumulative Fix 2017.06, and V8.5.6.0 through V8.5.6.0 CF2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158415. **CVE ID : CVE-2019-4149**	https://www.ibm.com/support/docview.wss?uid=ibm10885104	A-IBM-BUSI-230919/225
if.svnadmin_project					
if.svnadmin					
Cross-Site	06-09-2019	4.3	iF.SVNAdmin through 1.6.2	N/A	A-IF.-IF.S-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			allows svnadmin/usercreate.php CSRF to create a user. **CVE ID : CVE-2019-15128**		230919/226
image-rs					
image					
Use After Free	09-09-2019	7.5	An issue was discovered in the image crate before 0.21.3 for Rust, affecting the HDR image format decoder. Vec::set_len is called on an uninitialized vector, leading to a use-after-free and arbitrary code execution. **CVE ID : CVE-2019-16138**	N/A	A-IMA-IMAG-230919/227
instagram-php-api_project					
instagram-php-api					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-09-2019	4.3	cosenary Instagram-PHP-API (aka Instagram PHP API V2), as used in the UserPro plugin through 4.9.32 for WordPress, has XSS via the example/success.php error_description parameter. **CVE ID : CVE-2019-14470**	N/A	A-INS-INST-230919/228
isahc_project					
isahc					
Use After Free	09-09-2019	7.5	An issue was discovered in the chttp crate before 0.1.3 for Rust. There is a use-after-free during buffer conversion. **CVE ID : CVE-2019-16140**	N/A	A-ISA-ISAH-230919/229
Jenkins					
script_security					
Improper	12-09-2019	7.5	A sandbox bypass	N/A	A-JEN-SCRI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability in Jenkins Script Security Plugin 1.62 and earlier related to the handling of property names in property expressions in increment and decrement expressions allowed attackers to execute arbitrary code in sandboxed scripts. **CVE ID : CVE-2019-10399**		230919/230
Improper Input Validation	12-09-2019	7.5	A sandbox bypass vulnerability in Jenkins Script Security Plugin 1.62 and earlier related to the handling of subexpressions in increment and decrement expressions not involving actual assignment allowed attackers to execute arbitrary code in sandboxed scripts. **CVE ID : CVE-2019-10400**	N/A	A-JEN-SCRI-230919/231
Jetbrains					
teamcity					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-09-2019	4.3	JetBrains TeamCity 2019.1 and 2019.1.1 allows cross-site scripting (XSS), potentially making it possible to send an arbitrary HTTP request to a TeamCity server under the name of the currently logged-in user. **CVE ID : CVE-2019-15848**	https://blog.jetbrains.com/teamcity/2019/09/important-security-notice-xss-vulnerability-allowing-rce/	A-JET-TEAM-230919/232
jobberbase					
jobberbase					
Improper Neutralization of Special	08-09-2019	7.5	In Jobberbase 2.0, the parameter category is not sanitized in	N/A	A-JOB-JOBB-230919/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			public/page_subscribe.php, leading to /subscribe SQL injection. **CVE ID : CVE-2019-16125**		
kartatopia					
piluscart					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-09-2019	5	In Kartatopia PilusCart 1.4.1, the parameter filename in the file catalog.php is mishandled, leading to ../ Local File Disclosure. **CVE ID : CVE-2019-16123**	N/A	A-KAR-PILU-230919/234
kilo_project					
kilo					
Integer Overflow or Wraparound	08-09-2019	5	Kilo 0.0.1 has a heap-based buffer overflow because there is an integer overflow in a calculation involving the number of tabs in one row. **CVE ID : CVE-2019-16096**	N/A	A-KIL-KILO-230919/235
knowage-suite					
knowage					
N/A	05-09-2019	4	In Knowage through 6.1.1, an authenticated user that accesses the users page will obtain all user password hashes. **CVE ID : CVE-2019-13349**	N/A	A-KNO-KNOW-230919/236
Information Exposure	05-09-2019	5	In Knowage through 6.1.1, an unauthenticated user can enumerated valid usernames via the ChangePwdServlet page.	N/A	A-KNO-KNOW-230919/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-14278		
k-takata					
onigmo					
NULL Pointer Dereference	09-09-2019	5	Onigmo through 6.2.0 has a NULL pointer dereference in onig_error_code_to_str because of fetch_token in regparse.c. **CVE ID : CVE-2019-16161**	N/A	A-K-T-ONIG-230919/238
Out-of-bounds Read	09-09-2019	5	Onigmo through 6.2.0 has an out-of-bounds read in parse_char_class because of missing codepoint validation in regenc.c. **CVE ID : CVE-2019-16162**	N/A	A-K-T-ONIG-230919/239
larvit					
larvitbase					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-09-2019	5	An unintended require vulnerability in <v0.5.5 larvitbase-api may allow an attacker to load arbitrary non-production code (JavaScript file). **CVE ID : CVE-2019-5479**	N/A	A-LAR-LARV-230919/240
Lenovo					
xclarity_administrator					
Improper Restriction of XML External Entity Reference ('XXE')	03-09-2019	5	An XML External Entity (XXE) processing vulnerability was reported in Lenovo XClarity Administrator (LXCA) prior to version 2.5.0 , Lenovo XClarity Integrator (LXCI) for Microsoft System Center prior to version 7.7.0, and Lenovo XClarity Integrator	N/A	A-LEN-XCLA-230919/241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(LXCI) for VMWare vCenter prior to version 6.1.0 that could allow information disclosure. **CVE ID : CVE-2019-6179**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-09-2019	3.5	A stored cross-site scripting (XSS) vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.5.0 that could allow an administrative user to cause JavaScript code to be stored in LXCA which may then be executed in the user's web browser. The JavaScript code is not executed on LXCA itself. **CVE ID : CVE-2019-6180**	N/A	A-LEN-XCLA-230919/242
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-09-2019	4.3	A reflected cross-site scripting (XSS) vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.5.0 that could allow a crafted URL, if visited, to cause JavaScript code to be executed in the user's web browser. The JavaScript code is not executed on LXCA itself. **CVE ID : CVE-2019-6181**	N/A	A-LEN-XCLA-230919/243
Improper Neutralization of Special Elements in Output Used by a Downstream Component	03-09-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.5.0 that could allow an administrative user to store malformed data in LXCA Jobs and Event Log	N/A	A-LEN-XCLA-230919/244

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			data, that could result in crafted formulas stored in an exported CSV file. The crafted formula is not executed on LXCA itself. **CVE ID : CVE-2019-6182**		
libexpat_project					
libexpat					
Improper Restriction of XML External Entity Reference ('XXE')	04-09-2019	5	In libexpat before 2.2.8, crafted XML input could fool the parser into changing from DTD parsing to document parsing too early; a consecutive call to XML_GetCurrentLineNumber (or XML_GetCurrentColumnNumber) then resulted in a heap-based buffer over-read. **CVE ID : CVE-2019-15903**	N/A	A-LIB-LIBE-230919/245
librenms					
librenms					
Improper Input Validation	09-09-2019	7.5	An issue was discovered in LibreNMS through 1.47. The scripts that handle the graphing options (html/includes/graphs/common.inc.php and html/includes/graphs/graphs.inc.php) do not sufficiently validate or encode several fields of user supplied input. Some parameters are filtered with mysqli_real_escape_string, which is only useful for preventing SQL injection attacks; other parameters are unfiltered. This allows an	N/A	A-LIB-LIBR-230919/246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to inject RRDtool syntax with newline characters via the html/graph.php script. RRDtool syntax is quite versatile and an attacker could leverage this to perform a number of attacks, including disclosing directory structure and filenames, file content, denial of service, or writing arbitrary files. **CVE ID : CVE-2019-10665**		
Improper Control of Generation of Code ('Code Injection')	09-09-2019	6.8	An issue was discovered in LibreNMS through 1.47. Several of the scripts perform dynamic script inclusion via the include() function on user supplied input without sanitizing the values by calling basename() or a similar function. An attacker can leverage this to execute PHP code from the included file. Exploitation of these scripts is made difficult by additional text being appended (typically .inc.php), which means an attacker would need to be able to control both a filename and its content on the server. However, exploitation can be achieved as demonstrated by the csv.php?report=../ substring. **CVE ID : CVE-2019-10666**	N/A	A-LIB-LIBR-230919/247
Information Exposure	09-09-2019	5	An issue was discovered in LibreNMS through 1.47. Information disclosure can	N/A	A-LIB-LIBR-230919/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			occur: an attacker can fingerprint the exact code version installed and disclose local file paths. **CVE ID : CVE-2019-10667**		
Improper Authentication	09-09-2019	6.4	An issue was discovered in LibreNMS through 1.47. A number of scripts import the Authentication libraries, but do not enforce an actual authentication check. Several of these scripts disclose information or expose functions that are of a sensitive nature and are not expected to be publicly accessible. **CVE ID : CVE-2019-10668**	N/A	A-LIB-LIBR-230919/249
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-09-2019	6.5	An issue was discovered in LibreNMS through 1.47. There is a command injection vulnerability in html/includes/graphs/device/collectd.inc.php where user supplied parameters are filtered with the mysqli_escape_real_string function. This function is not the appropriate function to sanitize command arguments as it does not escape a number of command line syntax characters such as ` (backtick), allowing an attacker to inject commands into the variable $rrd_cmd, which gets executed via passthru(). **CVE ID : CVE-2019-10669**	N/A	A-LIB-LIBR-230919/250

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-09-2019	4.3	An issue was discovered in LibreNMS through 1.47. Many of the scripts rely on the function mysqli_escape_real_string for filtering data. However, this is particularly ineffective when returning user supplied input in an HTML or a JavaScript context, resulting in unsafe data being injected into these contexts, leading to attacker controlled JavaScript executing in the browser. One example of this is the string parameter in html/pages/inventory.inc.php. **CVE ID : CVE-2019-10670**	N/A	A-LIB-LIBR-230919/251
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-09-2019	6.5	An issue was discovered in LibreNMS through 1.47. It does not parameterize all user supplied input within database queries, resulting in SQL injection. An authenticated attacker can subvert these database queries to extract or manipulate data, as demonstrated by the graph.php sort parameter. **CVE ID : CVE-2019-10671**	N/A	A-LIB-LIBR-230919/252
Improper Control of Generation of Code ('Code Injection')	09-09-2019	6.5	An issue was discovered in LibreNMS 1.50.1. The scripts that handle graphing options (includes/html/graphs/common.inc.php and includes/html/graphs/graphs.inc.php) do not sufficiently validate or encode several	N/A	A-LIB-LIBR-230919/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fields of user supplied input. Some parameters are filtered with mysqli_real_escape_string, which is only useful for preventing SQL injection attacks; other parameters are unfiltered. This allows an attacker to inject RRDtool syntax with newline characters via the html/graph.php and html/graph-realtime.php scripts. RRDtool syntax is quite versatile and an attacker could leverage this to perform a number of attacks, including disclosing directory structure and filenames, disclosing file content, denial of service, or writing arbitrary files. NOTE: relative to CVE-2019-10665, this requires authentication and the pathnames differ. **CVE ID : CVE-2019-12463**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-09-2019	6	An issue was discovered in LibreNMS 1.50.1. An authenticated user can perform a directory traversal attack against the /pdf.php file with a partial filename in the report parameter, to cause local file inclusion resulting in code execution. **CVE ID : CVE-2019-12464**	N/A	A-LIB-LIBR-230919/254
Improper Neutralization of Special Elements	09-09-2019	5.5	An issue was discovered in LibreNMS 1.50.1. A SQL injection flaw was identified in the ajax_rulesuggest.php	N/A	A-LIB-LIBR-230919/255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			file where the term parameter is used insecurely in a database query for showing columns of a table, as demonstrated by an ajax_rulesuggest.php?debug=1&term= request. **CVE ID : CVE-2019-12465**		
Libreoffice					
libreoffice					
Improper Access Control	06-09-2019	7.5	LibreOffice has a feature where documents can specify that pre-installed macros can be executed on various script events such as mouse-over, document-open etc. Access is intended to be restricted to scripts under the share/Scripts/python, user/Scripts/python sub-directories of the LibreOffice install. Protection was added, to address CVE-2019-9852, to avoid a directory traversal attack where scripts in arbitrary locations on the file system could be executed by employing a URL encoding attack to defeat the path verification step. However this protection could be bypassed by taking advantage of a flaw in how LibreOffice assembled the final script URL location directly from components of the passed in path as opposed to solely from the sanitized output of the path verification step. This issue	https://www.libreoffice.org/about-us/security/advisories/CVE-2019-9854/	A-LIB-LIBR-230919/256

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects: Document Foundation LibreOffice 6.2 versions prior to 6.2.7; 6.3 versions prior to 6.3.1. **CVE ID : CVE-2019-9854**		
N/A	06-09-2019	7.5	LibreOffice is typically bundled with LibreLogo, a programmable turtle vector graphics script, which can execute arbitrary python commands contained with the document it is launched from. LibreOffice also has a feature where documents can specify that pre-installed scripts can be executed on various document script events such as mouse-over, etc. Protection was added to block calling LibreLogo from script event handers. However a Windows 8.3 path equivalence handling flaw left LibreOffice vulnerable under Windows that a document could trigger executing LibreLogo via a Windows filename pseudonym. This issue affects: Document Foundation LibreOffice 6.2 versions prior to 6.2.7; 6.3 versions prior to 6.3.1. **CVE ID : CVE-2019-9855**	https://www.libreoffice.org/about-us/security/advisories/CVE-2019-9855/	A-LIB-LIBR-230919/257
libslirp_project					
libslirp					
Use After Free	06-09-2019	5	libslirp 4.0.0, as used in QEMU 4.1.0, has a use-after-free in ip_reass in ip_input.c.	N/A	A-LIB-LIBS-230919/258

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15890		
Liferay					
liferay_portal					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-09-2019	4.3	Liferay Portal through 7.2.0 GA1 allows XSS via a journal article title to journal_article/page.jsp in journal/journal-taglib. **CVE ID : CVE-2019-16147**	N/A	A-LIF-LIFE-230919/259
lifterlms					
lifterlms					
Improper Privilege Management	10-09-2019	7.5	An issue was discovered in the LifterLMS plugin through 3.34.5 for WordPress. The upload_import function in the class.llms.admin.import.php script is prone to an unauthenticated options import vulnerability that could lead to privilege escalation (administrator account creation), website redirection, and stored XSS. **CVE ID : CVE-2019-15896**	N/A	A-LIF-LIFT-230919/260
Limesurvey					
limesurvey					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-09-2019	3.5	LimeSurvey before v3.17.14 allows stored XSS for escalating privileges from a low-privileged account to, for example, SuperAdmin. The attack uses a survey group in which the title contains JavaScript that is mishandled upon group deletion.	N/A	A-LIM-LIME-230919/261

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16172		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-09-2019	3.5	LimeSurvey before v3.17.14 allows reflected XSS for escalating privileges from a low-privileged account to, for example, SuperAdmin. This occurs in application/core/Survey_Common_Action.php, **CVE ID : CVE-2019-16173**	N/A	A-LIM-LIME-230919/262
Improper Restriction of XML External Entity Reference ('XXE')	09-09-2019	6.8	An XML injection vulnerability was found in Limesurvey before 3.17.14 that allows remote attackers to import specially crafted XML files and execute code or compromise data integrity. **CVE ID : CVE-2019-16174**	N/A	A-LIM-LIME-230919/263
Improper Restriction of Rendered UI Layers or Frames	09-09-2019	4.3	A clickjacking vulnerability was found in Limesurvey before 3.17.14. **CVE ID : CVE-2019-16175**	N/A	A-LIM-LIME-230919/264
Information Exposure	09-09-2019	5	A path disclosure vulnerability was found in Limesurvey before 3.17.14 that allows a remote attacker to discover the path to the application in the filesystem. **CVE ID : CVE-2019-16176**	N/A	A-LIM-LIME-230919/265
Information Exposure	09-09-2019	5	In Limesurvey before 3.17.14, the entire database is exposed through browser caching. **CVE ID : CVE-2019-16177**	N/A	A-LIM-LIME-230919/266
Improper Neutralization of Input	09-09-2019	3.5	A stored cross-site scripting (XSS) vulnerability was found in Limesurvey before 3.17.14	N/A	A-LIM-LIME-230919/267

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			that allows authenticated users with correct permissions to inject arbitrary web script or HTML via titles of admin box buttons on the home page. **CVE ID : CVE-2019-16178**		
Improper Certificate Validation	09-09-2019	5	Limesurvey before 3.17.14 does not enforce SSL/TLS usage in the default configuration. **CVE ID : CVE-2019-16179**	N/A	A-LIM-LIME-230919/268
Information Exposure	09-09-2019	5	Limesurvey before 3.17.14 allows remote attackers to bruteforce the login form and enumerate usernames when the LDAP authentication method is used. **CVE ID : CVE-2019-16180**	N/A	A-LIM-LIME-230919/269
Improper Input Validation	09-09-2019	4	In Limesurvey before 3.17.14, admin users can mark other users' notifications as read. **CVE ID : CVE-2019-16181**	N/A	A-LIM-LIME-230919/270
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-09-2019	4.3	A reflected cross-site scripting (XSS) vulnerability was found in Limesurvey before 3.17.14 that allows remote attackers to inject arbitrary web script or HTML via extensions of uploaded files. **CVE ID : CVE-2019-16182**	N/A	A-LIM-LIME-230919/271
Incorrect Default Permissions	09-09-2019	4	In Limesurvey before 3.17.14, admin users can run an integrity check without proper permissions.	N/A	A-LIM-LIME-230919/272

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16183		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-09-2019	7.5	A CSV injection vulnerability was found in Limesurvey before 3.17.14 that allows survey participants to inject commands via their survey responses that will be included in the export CSV file. **CVE ID : CVE-2019-16184**	N/A	A-LIM-LIME-230919/273
Incorrect Default Permissions	09-09-2019	6.5	In Limesurvey before 3.17.14, admin users can view, update, or delete reserved menu entries without proper permissions. **CVE ID : CVE-2019-16185**	N/A	A-LIM-LIME-230919/274
Incorrect Default Permissions	09-09-2019	6.5	In Limesurvey before 3.17.14, admin users can access the plugin manager without proper permissions. **CVE ID : CVE-2019-16186**	N/A	A-LIM-LIME-230919/275
Information Exposure	09-09-2019	5	Limesurvey before 3.17.14 uses an anti-CSRF cookie without the HttpOnly flag, which allows attackers to access a cookie value via a client-side script. **CVE ID : CVE-2019-16187**	N/A	A-LIM-LIME-230919/276
Mcafee					
enterprise_security_manager					
Improper Input Validation	11-09-2019	5	McAfee Web Gateway (MWG) earlier than 7.8.2.13 is vulnerable to a remote attacker exploiting CVE-2019-9511, potentially leading to a denial of service. This affects the scanning	https://kc.mcafee.com/corporate/index?page=content&id=SB10296	A-MCA-ENTE-230919/277

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			proxies. **CVE ID : CVE-2019-3643**		
Improper Input Validation	11-09-2019	5	McAfee Web Gateway (MWG) earlier than 7.8.2.13 is vulnerable to a remote attacker exploiting CVE-2019-9517, potentially leading to a denial of service. This affects the scanning proxies. **CVE ID : CVE-2019-3644**	https://kc.mcafee.com/corporate/index?page=content&id=SB10296	A-MCA-ENTE-230919/278
web_gateway					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-09-2019	4.3	Reflected Cross Site Scripting vulnerability in Administrators web console in McAfee Web Gateway (MWG) 7.8.x prior to 7.8.2.13 allows remote attackers to collect sensitive information or execute commands with the MWG administrator's credentials via tricking the administrator to click on a carefully constructed malicious link. **CVE ID : CVE-2019-3638**	https://kc.mcafee.com/corporate/index?page=content&id=SB10294	A-MCA-WEB_-230919/279
Improper Input Validation	11-09-2019	5	McAfee Web Gateway (MWG) earlier than 7.8.2.13 is vulnerable to a remote attacker exploiting CVE-2019-9511, potentially leading to a denial of service. This affects the scanning proxies. **CVE ID : CVE-2019-3643**	https://kc.mcafee.com/corporate/index?page=content&id=SB10296	A-MCA-WEB_-230919/280
Improper Input Validation	11-09-2019	5	McAfee Web Gateway (MWG) earlier than 7.8.2.13 is vulnerable to a remote	https://kc.mcafee.com/corporate/in	A-MCA-WEB_-230919/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker exploiting CVE-2019-9517, potentially leading to a denial of service. This affects the scanning proxies. **CVE ID : CVE-2019-3644**	dex?page=content&id=SB10296	
active_response					
Improper Input Validation	11-09-2019	5	McAfee Web Gateway (MWG) earlier than 7.8.2.13 is vulnerable to a remote attacker exploiting CVE-2019-9511, potentially leading to a denial of service. This affects the scanning proxies. **CVE ID : CVE-2019-3643**	https://kc.mcafee.com/corporate/index?page=content&id=SB10296	A-MCA-ACTI-230919/282
Improper Input Validation	11-09-2019	5	McAfee Web Gateway (MWG) earlier than 7.8.2.13 is vulnerable to a remote attacker exploiting CVE-2019-9517, potentially leading to a denial of service. This affects the scanning proxies. **CVE ID : CVE-2019-3644**	https://kc.mcafee.com/corporate/index?page=content&id=SB10296	A-MCA-ACTI-230919/283
advanced_threat_defense					
Improper Input Validation	11-09-2019	5	McAfee Web Gateway (MWG) earlier than 7.8.2.13 is vulnerable to a remote attacker exploiting CVE-2019-9511, potentially leading to a denial of service. This affects the scanning proxies. **CVE ID : CVE-2019-3643**	https://kc.mcafee.com/corporate/index?page=content&id=SB10296	A-MCA-ADVA-230919/284
Improper Input Validation	11-09-2019	5	McAfee Web Gateway (MWG) earlier than 7.8.2.13 is vulnerable to a remote	https://kc.mcafee.com/corporate/in	A-MCA-ADVA-230919/285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker exploiting CVE-2019-9517, potentially leading to a denial of service. This affects the scanning proxies. **CVE ID : CVE-2019-3644**	dex?page=content&id=SB10296	
mendix					
mendix					
Server-Side Request Forgery (SSRF)	10-09-2019	5	In Mendix 7.23.5 and earlier, issue in XML import mappings allow DOCTYPE declarations in the XML input that is potentially unsafe. **CVE ID : CVE-2019-12996**	https://docs.mendix.com/releasenotes/studio-pro/7.23#7236	A-MEN-MEND-230919/286
Microfocus					
service_manager_chat_server					
Information Exposure	10-09-2019	5	HTTP cookie in Micro Focus Service manager, Versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. And Micro Focus Service Manager Chat Server, versions 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. And Micro Focus Service Manager Chat Service 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. **CVE ID : CVE-2019-11668**	https://softwaresupport.softwaregrp.com/doc/KM03517335	A-MIC-SERV-230919/287
service_manager_chat_service					
Information Exposure	10-09-2019	5	HTTP cookie in Micro Focus Service manager, Versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. And Micro Focus Service Manager Chat Server, versions 9.41, 9.50, 9.51, 9.52, 9.60, 9.61,	https://softwaresupport.softwaregrp.com/doc/KM03517335	A-MIC-SERV-230919/288

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.62. And Micro Focus Service Manager Chat Service 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. **CVE ID : CVE-2019-11668**		
service_manager					
Information Exposure	10-09-2019	5	HTTP cookie in Micro Focus Service manager, Versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. And Micro Focus Service Manager Chat Server, versions 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. And Micro Focus Service Manager Chat Service 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. **CVE ID : CVE-2019-11668**	https://softwaresupport.softwaregrp.com/doc/KM03517335	A-MIC-SERV-230919/289
Incorrect Authorization	10-09-2019	5	Modifiable read only check box In Micro Focus Service Manager, versions 9.60p1, 9.61, 9.62. This vulnerability could be exploited to allow unauthorized modification of data. **CVE ID : CVE-2019-11669**	https://softwaresupport.softwaregrp.com/doc/KM03517334	A-MIC-SERV-230919/290
Microsoft					
lync					
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists in Lync 2013, aka 'Lync 2013 Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1209**	N/A	A-MIC-LYNC-230919/291
project_rome					
Improper	11-09-2019	4.3	An information disclosure	N/A	A-MIC-PROJ-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Certificate Validation			vulnerability exists in the way Rome SDK handles server SSL/TLS certificate validation, aka 'Rome SDK Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1231**		230919/292
visual_studio					
Improper Privilege Management	11-09-2019	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly impersonates certain file operations, aka 'Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1232**	N/A	A-MIC-VISU-230919/293
chakracore					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1217, CVE-2019-1237, CVE-2019-1298, CVE-2019-1300. **CVE ID : CVE-2019-1138**	N/A	A-MIC-CHAK-230919/294
Improper Restriction of Operations within the Bounds of a Memory	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is	N/A	A-MIC-CHAK-230919/295

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			unique from CVE-2019-1138, CVE-2019-1237, CVE-2019-1298, CVE-2019-1300. **CVE ID : CVE-2019-1217**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1138, CVE-2019-1217, CVE-2019-1298, CVE-2019-1300. **CVE ID : CVE-2019-1237**	N/A	A-MIC-CHAK-230919/296
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1138, CVE-2019-1217, CVE-2019-1237, CVE-2019-1300. **CVE ID : CVE-2019-1298**	N/A	A-MIC-CHAK-230919/297
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1138, CVE-2019-1217, CVE-2019-1237, CVE-2019-1298.	N/A	A-MIC-CHAK-230919/298

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1300		
edge					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1217, CVE-2019-1237, CVE-2019-1298, CVE-2019-1300. **CVE ID : CVE-2019-1138**	N/A	A-MIC-EDGE-230919/299
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1138, CVE-2019-1237, CVE-2019-1298, CVE-2019-1300. **CVE ID : CVE-2019-1217**	N/A	A-MIC-EDGE-230919/300
Incorrect Permission Assignment for Critical Resource	11-09-2019	4.3	A security feature bypass vulnerability exists when Microsoft Browsers fail to validate the correct Security Zone of requests for specific URLs, aka 'Microsoft Browser Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1220**	N/A	A-MIC-EDGE-230919/301
Improper Restriction of Operations	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in	N/A	A-MIC-EDGE-230919/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1138, CVE-2019-1217, CVE-2019-1298, CVE-2019-1300. **CVE ID : CVE-2019-1237**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1138, CVE-2019-1217, CVE-2019-1237, CVE-2019-1300. **CVE ID : CVE-2019-1298**	N/A	A-MIC-EDGE-230919/303
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when Microsoft Edge based on Edge HTML improperly handles objects in memory, aka 'Microsoft Edge based on Edge HTML Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1299**	N/A	A-MIC-EDGE-230919/304
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1138, CVE-2019-1217, CVE-2019-	N/A	A-MIC-EDGE-230919/305

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1237, CVE-2019-1298. **CVE ID : CVE-2019-1300**		
office					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1246**	N/A	A-MIC-OFFI-230919/306
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1263**	N/A	A-MIC-OFFI-230919/307
Improper Input Validation	11-09-2019	6.8	A security feature bypass vulnerability exists when Microsoft Office improperly handles input, aka 'Microsoft Office Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1264**	N/A	A-MIC-OFFI-230919/308
Improper Restriction of Operations within the	11-09-2019	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in	N/A	A-MIC-OFFI-230919/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1297**		
office_365_proplus					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1246**	N/A	A-MIC-OFFI-230919/310
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1263**	N/A	A-MIC-OFFI-230919/311
Improper Input Validation	11-09-2019	6.8	A security feature bypass vulnerability exists when Microsoft Office improperly handles input, aka 'Microsoft Office Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1264**	N/A	A-MIC-OFFI-230919/312
Improper Restriction of	11-09-2019	9.3	A remote code execution vulnerability exists in Microsoft Excel software	N/A	A-MIC-OFFI-230919/313

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1297**		
internet_explorer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1236. **CVE ID : CVE-2019-1208**	N/A	A-MIC-INTE-230919/314
Incorrect Permission Assignment for Critical Resource	11-09-2019	4.3	A security feature bypass vulnerability exists when Microsoft Browsers fail to validate the correct Security Zone of requests for specific URLs, aka 'Microsoft Browser Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1220**	N/A	A-MIC-INTE-230919/315
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2019-1221**	N/A	A-MIC-INTE-230919/316
.net_core					
Improper Input Validation	11-09-2019	5	A denial of service vulnerability exists when .NET Core improperly handles web requests, aka	N/A	A-MIC-.NET-230919/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'.NET Core Denial of Service Vulnerability'. **CVE ID : CVE-2019-1301**		
.net_framework					
Improper Privilege Management	11-09-2019	2.1	An elevation of privilege vulnerability exists when the .NET Framework common language runtime (CLR) allows file creation in arbitrary locations, aka '.NET Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1142**	N/A	A-MIC-.NET-230919/318
visual_studio_2017					
Improper Privilege Management	11-09-2019	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly impersonates certain file operations, aka 'Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1232**	N/A	A-MIC-VISU-230919/319
asp.net_core					
Improper Input Validation	11-09-2019	6.8	An elevation of privilege vulnerability exists when a ASP.NET Core web application, created using vulnerable project templates, fails to properly sanitize web requests, aka 'ASP.NET Core Elevation Of Privilege Vulnerability'. **CVE ID : CVE-2019-1302**	N/A	A-MIC-ASP.-230919/320
sharepoint_server					
Improper	11-09-2019	6.5	A remote code execution	N/A	A-MIC-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1295, CVE-2019-1296. **CVE ID : CVE-2019-1257**		SHAR-230919/321
Improper Privilege Management	11-09-2019	4	An elevation of privilege vulnerability exists in Microsoft SharePoint, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1260**	N/A	A-MIC-SHAR-230919/322
Cross-Site Request Forgery (CSRF)	11-09-2019	6.8	A spoofing vulnerability exists in Microsoft SharePoint when it improperly handles requests to authorize applications, resulting in cross-site request forgery (CSRF).To exploit this vulnerability, an attacker would need to create a page specifically designed to cause a cross-site request, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1259. **CVE ID : CVE-2019-1261**	N/A	A-MIC-SHAR-230919/323
Improper Input Validation	11-09-2019	6.5	A remote code execution vulnerability exists in Microsoft SharePoint where APIs aren't properly protected from unsafe data	N/A	A-MIC-SHAR-230919/324

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1257, CVE-2019-1296. **CVE ID : CVE-2019-1295**		
Improper Input Validation	11-09-2019	6.5	A remote code execution vulnerability exists in Microsoft SharePoint where APIs aren't properly protected from unsafe data input, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1257, CVE-2019-1295. **CVE ID : CVE-2019-1296**	N/A	A-MIC-SHAR-230919/325
sharepoint_enterprise_server					
Improper Input Validation	11-09-2019	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1295, CVE-2019-1296. **CVE ID : CVE-2019-1257**	N/A	A-MIC-SHAR-230919/326
Improper Privilege Management	11-09-2019	4	An elevation of privilege vulnerability exists in Microsoft SharePoint, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1260**	N/A	A-MIC-SHAR-230919/327
Cross-Site	11-09-2019	6.8	A spoofing vulnerability	N/A	A-MIC-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			exists in Microsoft SharePoint when it improperly handles requests to authorize applications, resulting in cross-site request forgery (CSRF).To exploit this vulnerability, an attacker would need to create a page specifically designed to cause a cross-site request, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1259. **CVE ID : CVE-2019-1261**		SHAR-230919/328
Improper Input Validation	11-09-2019	6.5	A remote code execution vulnerability exists in Microsoft SharePoint where APIs aren't properly protected from unsafe data input, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1257, CVE-2019-1296. **CVE ID : CVE-2019-1295**	N/A	A-MIC-SHAR-230919/329
Improper Input Validation	11-09-2019	6.5	A remote code execution vulnerability exists in Microsoft SharePoint where APIs aren't properly protected from unsafe data input, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1257, CVE-2019-1295. **CVE ID : CVE-2019-1296**	N/A	A-MIC-SHAR-230919/330
exchange_server					
Improper	11-09-2019	7.8	A denial of service	N/A	A-MIC-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists in Microsoft Exchange Server software when the software fails to properly handle objects in memory, aka 'Microsoft Exchange Denial of Service Vulnerability'. **CVE ID : CVE-2019-1233**		EXCH-230919/331
Improper Input Validation	11-09-2019	4.3	A spoofing vulnerability exists in Microsoft Exchange Server when Outlook Web App (OWA) fails to properly handle web requests, aka 'Microsoft Exchange Spoofing Vulnerability'. **CVE ID : CVE-2019-1266**	N/A	A-MIC-EXCH-230919/332
sharepoint_foundation					
Improper Input Validation	11-09-2019	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1295, CVE-2019-1296. **CVE ID : CVE-2019-1257**	N/A	A-MIC-SHAR-230919/333
Cross-Site Request Forgery (CSRF)	11-09-2019	6.8	A spoofing vulnerability exists in Microsoft SharePoint when it improperly handles requests to authorize applications, resulting in cross-site request forgery (CSRF).To exploit this vulnerability, an attacker would need to create a page specifically	N/A	A-MIC-SHAR-230919/334

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			designed to cause a cross-site request, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1261. **CVE ID : CVE-2019-1259**		
Improper Privilege Management	11-09-2019	4	An elevation of privilege vulnerability exists in Microsoft SharePoint, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1260**	N/A	A-MIC-SHAR-230919/335
Cross-Site Request Forgery (CSRF)	11-09-2019	6.8	A spoofing vulnerability exists in Microsoft SharePoint when it improperly handles requests to authorize applications, resulting in cross-site request forgery (CSRF).To exploit this vulnerability, an attacker would need to create a page specifically designed to cause a cross-site request, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1259. **CVE ID : CVE-2019-1261**	N/A	A-MIC-SHAR-230919/336
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. **CVE ID : CVE-2019-1262**	N/A	A-MIC-SHAR-230919/337

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	11-09-2019	6.5	A remote code execution vulnerability exists in Microsoft SharePoint where APIs aren't properly protected from unsafe data input, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1257, CVE-2019-1296. **CVE ID : CVE-2019-1295**	N/A	A-MIC-SHAR-230919/338
Improper Input Validation	11-09-2019	6.5	A remote code execution vulnerability exists in Microsoft SharePoint where APIs aren't properly protected from unsafe data input, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1257, CVE-2019-1295. **CVE ID : CVE-2019-1296**	N/A	A-MIC-SHAR-230919/339
powershell_core					
Improper Input Validation	11-09-2019	5	A denial of service vulnerability exists when .NET Core improperly handles web requests, aka '.NET Core Denial of Service Vulnerability'. **CVE ID : CVE-2019-1301**	N/A	A-MIC-POWE-230919/340
team_foundation_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site	11-09-2019	3.5	A Cross-site Scripting (XSS) vulnerability exists when Team Foundation Server does not properly sanitize user provided input, aka 'Team Foundation Server Cross-site Scripting	N/A	A-MIC-TEAM-230919/341

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			Vulnerability'. **CVE ID : CVE-2019-1305**		
Improper Input Validation	11-09-2019	7.5	A remote code execution vulnerability exists when Azure DevOps Server (ADO) and Team Foundation Server (TFS) fail to validate input properly, aka 'Azure DevOps and Team Foundation Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1306**	N/A	A-MIC-TEAM-230919/342
excel					
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1263**	N/A	A-MIC-EXCE-230919/343
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1297**	N/A	A-MIC-EXCE-230919/344
visual_studio_2019					
Improper Privilege Management	11-09-2019	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly impersonates certain file operations, aka 'Diagnostics Hub Standard Collector	N/A	A-MIC-VISU-230919/345

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1232**		
project					
Improper Input Validation	11-09-2019	6.8	A security feature bypass vulnerability exists when Microsoft Office improperly handles input, aka 'Microsoft Office Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1264**	N/A	A-MIC-PROJ-230919/346
yammer					
Improper Input Validation	11-09-2019	5	A security feature bypass vulnerability exists when Microsoft Yammer App for Android fails to apply the correct Intune MAM Policy.This could allow an attacker to perform functions that are restricted by Intune Policy.The security update addresses the vulnerability by correcting the way the policy is applied to Yammer App., aka 'Microsoft Yammer Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1265**	N/A	A-MIC-YAMM-230919/347
Misp					
misp					
Improper Privilege Management	10-09-2019	4	MISP before 2.4.115 allows privilege escalation in certain situations. After updating to 2.4.115, escalation attempts are blocked by the __checkLoggedActions function with a "This could be an indication of an	N/A	A-MIS-MISP-230919/348

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attempted privilege escalation on older vulnerable versions of MISP (<2.4.115)" message. **CVE ID : CVE-2019-16202**		
msi					
afterburner					
Improper Privilege Management	11-09-2019	7.2	The driver in Micro-Star MSI Afterburner 4.6.2.15658 (aka RTCore64.sys and RTCore32.sys) allows any authenticated user to read and write to arbitrary memory, I/O ports, and MSRs. This can be exploited for privilege escalation, code execution under high privileges, and information disclosure. These signed drivers can also be used to bypass the Microsoft driver-signing policy to deploy malicious code. **CVE ID : CVE-2019-16098**	N/A	A-MSI-AFTE-230919/349
myhtml_project					
myhtml					
NULL Pointer Dereference	09-09-2019	4.3	MyHTML through 4.0.5 has a NULL pointer dereference in myhtml_tree_node_remove in tree.c. **CVE ID : CVE-2019-16164**	N/A	A-MYH-MYHT-230919/350
Nagios					
log_server					
Improper Neutralization of Input During Web	03-09-2019	4.3	Nagios Log Server before 2.0.8 allows Reflected XSS via the username on the Login page.	N/A	A-NAG-LOG_-230919/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2019-15898**		
nagios_xi					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-09-2019	9	Nagios XI before 5.6.6 allows remote command execution as root. The exploit requires access to the server as the nagios user, or access as the admin user via the web interface. The getprofile.sh script, invoked by downloading a system profile (profile.php?cmd=download) , is executed as root via a passwordless sudo entry; the script executes check_plugin, which is owned by the nagios user. A user logged into Nagios XI with permissions to modify plugins, or the nagios user on the server, can modify the check_plugin executable and insert malicious commands to execute as root. **CVE ID : CVE-2019-15949**	N/A	A-NAG-NAGI-230919/352
Naver					
cloud_explorer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-09-2019	5	NDrive(1.2.2).sys in Naver Cloud Explorer has a stack-based buffer overflow, which allows attackers to cause a denial of service when reading data from IOCTL handle. **CVE ID : CVE-2019-13156**	https://cve.naver.com/detail/cve-2019-13156	A-NAV-CLOU-230919/353

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Netapp					
oncommand_workflow_automation					
Information Exposure	10-09-2019	5	OnCommand Workflow Automation versions prior to 5.0 shipped without certain HTTP Security headers configured which could allow an attacker to obtain sensitive information via unspecified vectors. **CVE ID : CVE-2019-5503**	https://security.netapp.com/advisory/ntap-20190909-0001/	A-NET-ONCO-230919/354
nic					
bird					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-09-2019	5	BIRD Internet Routing Daemon 1.6.x through 1.6.7 and 2.x through 2.0.5 has a stack-based buffer overflow. The BGP daemon's support for RFC 8203 administrative shutdown communication messages included an incorrect logical expression when checking the validity of an input message. Sending a shutdown communication with a sufficient message length causes a four-byte overflow to occur while processing the message, where two of the overflow bytes are attacker-controlled and two are fixed. **CVE ID : CVE-2019-16159**	N/A	A-NIC-BIRD-230919/355
oceanwp					
ocean_extra					
Improper Input Validation	11-09-2019	5	includes/wizard/wizard.php in the Ocean Extra plugin through 1.5.8 for WordPress	N/A	A-OCE-OCEA-230919/356

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated options changes and injection of a Cascading Style Sheets (CSS) token sequence. **CVE ID : CVE-2019-16250**		
once_cell_project					
once_cell					
Improper Input Validation	09-09-2019	5	An issue was discovered in the once_cell crate before 1.0.1 for Rust. There is a panic during initialization of Lazy. **CVE ID : CVE-2019-16141**	N/A	A-ONC-ONCE-230919/357
oniguruma_project					
oniguruma					
Uncontrolled Resource Consumption	09-09-2019	5	Oniguruma before 6.9.3 allows Stack Exhaustion in regcomp.c because of recursion in regparse.c. **CVE ID : CVE-2019-16163**	N/A	A-ONI-ONIG-230919/358
Opencv					
opencv					
Divide By Zero	05-09-2019	5	An issue was discovered in OpenCV 4.1.0. There is a divide-by-zero error in cv::HOGDescriptor::getDescriptorSize in modules/objdetect/src/hog.cpp. **CVE ID : CVE-2019-15939**	N/A	A-OPE-OPEN-230919/359
Out-of-bounds Read	11-09-2019	7.5	OpenCV 4.1.1 has an out-of-bounds read in hal_baseline::v_load in core/hal/intrin_sse.hpp when called from computeSSDMeanNorm in modules/video/src/dis_flow.	N/A	A-OPE-OPEN-230919/360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cpp. **CVE ID : CVE-2019-16249**		
opensc_project					
opensc					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-09-2019	7.5	OpenSC before 0.20.0-rc1 has an out-of-bounds access of an ASN.1 Bitstring in decode_bit_string in libopensc/asn1.c. **CVE ID : CVE-2019-15945**	N/A	A-OPE-OPEN-230919/361
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-09-2019	7.5	OpenSC before 0.20.0-rc1 has an out-of-bounds access of an ASN.1 Octet string in asn1_decode_entry in libopensc/asn1.c. **CVE ID : CVE-2019-15946**	N/A	A-OPE-OPEN-230919/362
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-09-2019	5	An issue was discovered in the pam_p11 component 0.2.0 and 0.3.0 for OpenSC. If a smart card creates a signature with a length longer than 256 bytes, this triggers a buffer overflow. This may be the case for RSA keys with 4096 bits depending on the signature scheme. **CVE ID : CVE-2019-16058**	N/A	A-OPE-OPEN-230919/363
Openssl					
openssl					
Missing Encryption of Sensitive Data	10-09-2019	1.9	Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant	https://www.openssl.org/news/secadv/201909	A-OPE-OPEN-230919/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s). **CVE ID : CVE-2019-1547**	10.txt	
Use of Insufficiently Random Values	10-09-2019	5	OpenSSL 1.1.1 introduced a rewritten random number generator (RNG). This was intended to include protection in the event of a fork() system call in order to	https://www.openssl.org/news/secadv/20190910.txt	A-OPE-OPEN-230919/365

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ensure that the parent and child processes did not share the same RNG state. However this protection was not being used in the default case. A partial mitigation for this issue is that the output from a high precision timer is mixed into the RNG state so the likelihood of a parent and child process sharing state is significantly reduced. If an application already calls OPENSSL_init_crypto() explicitly using OPENSSL_INIT_ATFORK then this problem does not occur at all. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). **CVE ID : CVE-2019-1549**		
Missing Encryption of Sensitive Data	10-09-2019	4.3	In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient	https://www.openssl.org/news/secadv/20190910.txt	A-OPE-OPEN-230919/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s). **CVE ID : CVE-2019-1563**		
Opmantek					
open-audit					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	13-09-2019	6.5	The Create Discoveries feature of Open-AudIT before 3.2.0 allows an authenticated attacker to execute arbitrary OS commands via a crafted value for a URL field. **CVE ID : CVE-2019-16293**	N/A	A-OPM-OPEN-230919/367
padrinorb					
padrino-contrib					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-09-2019	4.3	The breadcrumbs contributed module through 0.2.0 for Padrino Framework allows XSS via a caption. **CVE ID : CVE-2019-16145**	N/A	A-PAD-PADR-230919/368
Panasonic					
video_insight_vms					
Improper Neutralization of Special Elements used in an SQL Command	12-09-2019	6.5	SQL injection vulnerability in the Video Insight VMS 7.3.2.5 and earlier allows remote authenticated attackers to execute arbitrary SQL commands via unspecified vectors.	N/A	A-PAN-VIDE-230919/369

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2019-5996**		
pengutronix					
barebox					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-09-2019	7.5	Pengutronix barebox through 2019.08.1 has a remote buffer overflow in nfs_readlink_reply in net/nfs.c because a length field is directly used for a memcpy. **CVE ID : CVE-2019-15937**	N/A	A-PEN-BARE-230919/370
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-09-2019	7.5	Pengutronix barebox through 2019.08.1 has a remote buffer overflow in nfs_readlink_req in fs/nfs.c because a length field is directly used for a memcpy. **CVE ID : CVE-2019-15938**	N/A	A-PEN-BARE-230919/371
Phpmyadmin					
phpmyadmin					
Cross-Site Request Forgery (CSRF)	13-09-2019	5.8	A CSRF issue in phpMyAdmin 4.9.0.1 allows deletion of any server in the Setup page. **CVE ID : CVE-2019-12922**	N/A	A-PHP-PHPM-230919/372
phpok					
oklite					
Unrestricted Upload of File with Dangerous Type	08-09-2019	6.5	framework/admin/modulec_control.php in OKLite v1.2.25 has an Arbitrary File Upload Vulnerability because a .php file from a ZIP archive can be written to /data/cache/. **CVE ID : CVE-2019-16131**	N/A	A-PHP-OKLI-230919/373
Improper Limitation of	08-09-2019	5.5	An issue was discovered in OKLite v1.2.25.	N/A	A-PHP-OKLI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			framework/admin/tpl_control.php allows remote attackers to delete arbitrary files via a title directory-traversal pathname followed by a crafted substring. **CVE ID : CVE-2019-16132**		230919/374
Piwigo					
piwigo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-09-2019	6.8	admin.php?page=notification_by_mail in Piwigo 2.9.5 has XSS via the nbm&#95;send&#95;html&#95;mail, nbm&#95;send&#95;mail&#95;as, nbm&#95;send&#95;detailed&#95;content, nbm&#95;complementary&#95;mail&#95;content, nbm&#95;send&#95;recent&#95;post&#95;dates, or param&#95;submit parameter. This is exploitable via CSRF. **CVE ID : CVE-2019-13363**	N/A	A-PIW-PIWI-230919/375
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-09-2019	6.8	admin.php?page=account_billing in Piwigo 2.9.5 has XSS via the vat&#95;number, billing&#95;name, company, or billing&#95;address parameter. This is exploitable via CSRF. **CVE ID : CVE-2019-13364**	N/A	A-PIW-PIWI-230919/376
Plataformatec					
devise					
Improper Input	08-09-2019	5	An issue was discovered in Plataformatec Devise before	N/A	A-PLA-DEVI-230919/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			4.7.1. It confirms accounts upon receiving a request with a blank confirmation_token, if a database record has a blank value in the confirmation_token column. (However, there is no scenario within Devise itself in which such database records would exist.) **CVE ID : CVE-2019-16109**		
profilegrid					
profilegrid					
Improper Control of Generation of Code ('Code Injection')	03-09-2019	6.5	The profilegrid-user-profiles-groups-and-communities plugin before 2.8.6 for WordPress has remote code execution via an wp-admin/admin-ajax.php request with the action=pm_template_preview &html=<?php substring followed by PHP code. **CVE ID : CVE-2019-15873**	N/A	A-PRO-PROF-230919/378
py-lmdb_project					
py-lmdb					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.5	An issue was discovered in py-lmdb 0.97. For certain values of md_flags, mdb_node_add does not properly set up a memcpy destination, leading to an invalid write operation. **CVE ID : CVE-2019-16224**	N/A	A-PY--PY-L-230919/379
Improper Restriction of	11-09-2019	7.5	An issue was discovered in py-lmdb 0.97. For certain values of mp_flags,	N/A	A-PY--PY-L-230919/380

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			mdb_page_touch does not properly set up mc->mc_pg[mc->top], leading to an invalid write operation. **CVE ID : CVE-2019-16225**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	5	An issue was discovered in py-lmdb 0.97. mdb_node_del does not validate a memmove in the case of an unexpected node->mn_hi, leading to an invalid write operation. **CVE ID : CVE-2019-16226**	N/A	A-PY--PY-L-230919/381
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.5	An issue was discovered in py_lmdb 0.97. For certain values of mn_flags, mdb_cursor_set triggers a memcpy with an invalid write operation within mdb_xcursor_init1. **CVE ID : CVE-2019-16227**	N/A	A-PY--PY-L-230919/382
Divide By Zero	11-09-2019	5	An issue was discovered in py-lmdb 0.97. There is a divide-by-zero error in the function mdb_env_open2 if mdb_env_read_header obtains a zero value for a certain size field. **CVE ID : CVE-2019-16228**	N/A	A-PY--PY-L-230919/383
Python					
python					
Improper Input Validation	06-09-2019	5	An issue was discovered in Python through 2.7.16, 3.x through 3.5.7, 3.6.x through 3.6.9, and 3.7.x through 3.7.4. The email module wrongly parses email addresses that contain multiple @	N/A	A-PYT-PYTH-230919/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied. An attack may be the same as in CVE-2019-11340; however, this CVE applies to Python more generally. **CVE ID : CVE-2019-16056**		
Qemu					
qemu					
Use After Free	06-09-2019	5	libslirp 4.0.0, as used in QEMU 4.1.0, has a use-after-free in ip_reass in ip_input.c. **CVE ID : CVE-2019-15890**	N/A	A-QEM-QEMU-230919/385
rancher					
rancher					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-09-2019	4.3	Rancher 2 through 2.2.4 is vulnerable to a Cross-Site Websocket Hijacking attack that allows an exploiter to gain access to clusters managed by Rancher. The attack requires a victim to be logged into a Rancher server, and then to access a third-party site hosted by the exploiter. Once that is accomplished, the exploiter is able to execute commands against the cluster's Kubernetes API with the permissions and identity of the victim. **CVE ID : CVE-2019-13209**	https://forums.rancher.com/t/rancher-release-v2-2-5-addresses-rancher-cve-2019-13209/14801	A-RAN-RANC-230919/386

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redhat					
virtualization_host					
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073. **CVE ID : CVE-2019-1125**	N/A	A-RED-VIRT-230919/387
openshift					
Information Exposure Through Log Files	04-09-2019	1.9	On version 1.9.0, If DEBUG logging is enable, F5 Container Ingress Service (CIS) for Kubernetes and Red Hat OpenShift (k8s-bigip-ctlr) log files may contain BIG-IP secrets such as SSL Private Keys and Private key Passphrases as provided as inputs by an AS3 Declaration. **CVE ID : CVE-2019-6648**	N/A	A-RED-OPEN-230919/388
renderdocs-rs_project					
renderdocs-rs					
Improper Input Validation	09-09-2019	7.5	An issue was discovered in the renderdoc crate before 0.5.0 for Rust. Multiple exposed methods take self by immutable reference, which is incompatible with a multi-threaded application. **CVE ID : CVE-2019-16142**	N/A	A-REN-REND-230919/389
sahipro					
sahi_pro					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	06-09-2019	7.5	An issue was discovered in Tyto Sahi Pro 6.x through 8.0.0. TestRunner_Non_distributed (and distributed end points) does not have any authentication mechanism. This allow an attacker to execute an arbitrary script on the remote Sahi Pro server. There is also a password-protected web interface intended for remote access to scripts. This web interface lacks server-side validation, which allows an attacker to create/modify/delete a script remotely without any password. Chaining both of these issues results in remote code execution on the Sahi Pro server. **CVE ID : CVE-2019-15102**	N/A	A-SAH-SAHI-230919/390
sakailms					
sakai					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-09-2019	4.3	Sakai through 12.6 allows XSS via a chat user name. **CVE ID : CVE-2019-16148**	N/A	A-SAK-SAKA-230919/391
Samba					
samba					
Improper Limitation of a Pathname to a	03-09-2019	6.4	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3,	N/A	A-SAM-SAMB-230919/392

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share. **CVE ID : CVE-2019-10197**		
SAP					
netweaver_process_integration					
Information Exposure	10-09-2019	4	Under certain conditions SAP NetWeaver Process Integration Runtime Workbench ? MESSAGING and SAP_XIAF (before versions 7.31, 7.40, 7.50) allows an attacker to access information which would otherwise be restricted. **CVE ID : CVE-2019-0356**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=525962506	A-SAP-NETW-230919/393
hana					
Improper Privilege Management	10-09-2019	7.2	The administrator of SAP HANA database, before versions 1.0 and 2.0, can misuse HANA to execute commands with operating system "root" privileges. **CVE ID : CVE-2019-0357**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=525962506	A-SAP-HANA-230919/394
netweaver_application_server_java					
Improper Control of Generation of Code ('Code Injection')	10-09-2019	6.5	SAP NetWeaver Application Server Java Web Container, ENGINEAPI (before versions 7.10, 7.20, 7.30, 7.31, 7.40, 7.50) and SAP-JEECOR (before versions 6.40, 7.0, 7.01), allows an attacker to inject code that can be	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=525962506	A-SAP-NETW-230919/395

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executed by the application. An attacker could thereby control the behaviour of the application. **CVE ID : CVE-2019-0355**		
businessobjects_business_intelligence_platform					
Information Exposure	10-09-2019	5	In SAP Business Objects Business Intelligence Platform, before versions 4.1, 4.2 and 4.3, some dynamic pages (like jsp) are cached, which leads to an attacker can see the sensitive information via cache and can open the dynamic pages even after logout. **CVE ID : CVE-2019-0352**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=525962506	A-SAP-BUSI-230919/396
business_one_client					
Information Exposure	10-09-2019	2.1	Under certain conditions SAP Business One client (B1_ON_HANA, SAP-M-BO), before versions 9.2 and 9.3, allows an attacker to access information which would otherwise be restricted. **CVE ID : CVE-2019-0353**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=525962506	A-SAP-BUSI-230919/397
supplier_relationship_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-09-2019	4.3	SAP Supplier Relationship Management (Master Data Management Catalog - SRM_MDM_CAT, before versions 3.73, 7.31, 7.32) does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2019-0361**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=525962506	A-SAP-SUPP-230919/398

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sap_kernel_krnl32nuc					
Uncontrolled Resource Consumption	10-09-2019	7.8	SAP Kernel (RFC), KRNL32NUC, KRNL32UC and KRNL64NUC before versions 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64UC, before versions 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73 and KERNEL before versions 7.21, 7.49, 7.53, 7.73, 7.76 SAP GUI for Windows (BC-FES-GUI) before versions 7.5, 7.6, and SAP GUI for Java (BC-FES-JAV) before version 7.5, allow an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service. **CVE ID : CVE-2019-0365**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=525962506	A-SAP-SAP_-230919/399
sap_kernel_krnl32uc					
Uncontrolled Resource Consumption	10-09-2019	7.8	SAP Kernel (RFC), KRNL32NUC, KRNL32UC and KRNL64NUC before versions 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64UC, before versions 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73 and KERNEL before versions 7.21, 7.49, 7.53, 7.73, 7.76 SAP GUI for Windows (BC-FES-GUI) before versions 7.5, 7.6, and SAP GUI for Java (BC-FES-JAV) before version 7.5, allow an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service.	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=525962506	A-SAP-SAP_-230919/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0365		
sap_kernel_krnl64nuc					
Uncontrolled Resource Consumption	10-09-2019	7.8	SAP Kernel (RFC), KRNL32NUC, KRNL32UC and KRNL64NUC before versions 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64UC, before versions 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73 and KERNEL before versions 7.21, 7.49, 7.53, 7.73, 7.76 SAP GUI for Windows (BC-FES-GUI) before versions 7.5, 7.6, and SAP GUI for Java (BC-FES-JAV) before version 7.5, allow an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service. **CVE ID : CVE-2019-0365**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=525962506	A-SAP-SAP_-230919/401
sap_kernel_krnl64uc					
Uncontrolled Resource Consumption	10-09-2019	7.8	SAP Kernel (RFC), KRNL32NUC, KRNL32UC and KRNL64NUC before versions 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64UC, before versions 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73 and KERNEL before versions 7.21, 7.49, 7.53, 7.73, 7.76 SAP GUI for Windows (BC-FES-GUI) before versions 7.5, 7.6, and SAP GUI for Java (BC-FES-JAV) before version 7.5, allow an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=525962506	A-SAP-SAP_-230919/402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service. **CVE ID : CVE-2019-0365**		
hana_extended_application_services					
Improper Input Validation	10-09-2019	5.5	Attackers may misuse an HTTP/REST endpoint of SAP HANA Extended Application Services (Advanced model), before version 1.0.118, to overload the server or retrieve information about internal network ports. **CVE ID : CVE-2019-0363**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=525962506	A-SAP-HANA-230919/403
Improper Input Validation	10-09-2019	4	Attackers may misuse an HTTP/REST endpoint of SAP HANA Extended Application Services (Advanced model), before version 1.0.118, to enumerate open ports. **CVE ID : CVE-2019-0364**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=525962506	A-SAP-HANA-230919/404
sap_kernel					
Uncontrolled Resource Consumption	10-09-2019	7.8	SAP Kernel (RFC), KRNL32NUC, KRNL32UC and KRNL64NUC before versions 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64UC, before versions 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73 and KERNEL before versions 7.21, 7.49, 7.53, 7.73, 7.76 SAP GUI for Windows (BC-FES-GUI) before versions 7.5, 7.6, and SAP GUI for Java (BC-FES-JAV) before version 7.5, allow an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service.	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=525962506	A-SAP-SAP_-230919/405

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0365		
sapplica					
sentrifugo					
Cross-Site Request Forgery (CSRF)	06-09-2019	6.8	Sentrifugo 3.2 lacks CSRF protection. This could lead to an attacker tricking the administrator into executing arbitrary code at index.php/dashboard/viewprofile via a crafted HTML page. **CVE ID : CVE-2019-16059**	N/A	A-SAP-SENT-230919/406
search_exclude_project					
search_exclude					
Improper Access Control	09-09-2019	5	search-exclude.php in the "Search Exclude" plugin before 1.2.4 for WordPress allows unauthenticated options changes. **CVE ID : CVE-2019-15895**	N/A	A-SEA-SEAR-230919/407
senecajs					
seneca					
Information Exposure Through an Error Message	09-09-2019	5	Seneca < 3.9.0 contains a vulnerability that could lead to exposing environment variables to unauthorized users. **CVE ID : CVE-2019-5483**	N/A	A-SEN-SENE-230919/408
sentrifugo					
sentrifugo					
Improper Control of Generation of Code ('Code Injection')	04-09-2019	6.5	Multiple file upload restriction bypass vulnerabilities in Sentrifugo 3.2 could allow authenticated users to execute arbitrary code via a webshell.	N/A	A-SEN-SENT-230919/409

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15813		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-09-2019	3.5	Multiple stored XSS vulnerabilities in Sentrifugo 3.2 could allow authenticated users to inject arbitrary web script or HTML. **CVE ID : CVE-2019-15814**	N/A	A-SEN-SENT-230919/410
slickquiz_project					
slickquiz					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-09-2019	6.5	The slickquiz plugin through 1.3.7.1 for WordPress allows SQL Injection by Subscriber users, as demonstrated by a /wp-admin/admin.php?page=slickquiz-scores&id= or /wp-admin/admin.php?page=slickquiz-edit&id= or /wp-admin/admin.php?page=slickquiz-preview&id= URI. **CVE ID : CVE-2019-12516**	N/A	A-SLI-SLIC-230919/411
Sonatype					
nexus_repository_manager					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-09-2019	9	The Nexus Yum Repository Plugin in v2 is vulnerable to Remote Code Execution when instances using CommandLineExecutor.java are supplied vulnerable data, such as the Yum Configuration Capability. **CVE ID : CVE-2019-5475**	N/A	A-SON-NEXU-230919/412
spin-rs_project					
spin-rs					
Improper	09-09-2019	7.8	An issue was discovered in	N/A	A-SPI-SPIN-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			the spin crate before 0.5.2 for Rust, when RwLock is used. Because memory ordering is mishandled, two writers can acquire the lock at the same time, violating mutual exclusion. **CVE ID : CVE-2019-16137**		230919/413
Sqlite					
sqlite					
Divide By Zero	09-09-2019	5	In SQLite through 3.29.0, whereLoopAddBtreeIndex in sqlite3.c can crash a browser or other application because of missing validation of a sqlite_stat1 sz field, aka a "severe division by zero in the query planner." **CVE ID : CVE-2019-16168**	N/A	A-SQL-SQLI-230919/414
ss-proj					
shirasagi					
URL Redirection to Untrusted Site ('Open Redirect')	12-09-2019	5.8	Open redirect vulnerability in SHIRASAGI v1.7.0 and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors. **CVE ID : CVE-2019-6009**	N/A	A-SS--SHIR-230919/415
statichttpserver_project					
statichttpserver					
Improper Limitation of a Pathname to a Restricted Directory	03-09-2019	5	A path traversal vulnerability in <= v0.9.7 of statichttpserver npm module allows attackers to list files in arbitrary folders. **CVE ID : CVE-2019-5480**	N/A	A-STA-STAT-230919/416

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')					
supervisord					
supervisor					
Missing Authentication for Critical Function	10-09-2019	6.4	In supervisord in Supervisor through 4.0.2, an unauthenticated user can read log files or restart a service. WARNING: This issue will not be fixed by the maintainer. The ability to run an open server will not be removed because users often use it for local development, therefore no action will be taken. **CVE ID : CVE-2019-12105**	N/A	A-SUP-SUPE-230919/417
symonics					
libmysofa					
Out-of-bounds Read	07-09-2019	5	Symonics libmysofa 0.7 has an out-of-bounds read in directblockRead in hdf/fractalhead.c. **CVE ID : CVE-2019-16091**	N/A	A-SYM-LIBM-230919/418
NULL Pointer Dereference	07-09-2019	7.5	Symonics libmysofa 0.7 has a NULL pointer dereference in getHrtf in hrtf/reader.c. **CVE ID : CVE-2019-16092**	N/A	A-SYM-LIBM-230919/419
Out-of-bounds Write	07-09-2019	7.5	Symonics libmysofa 0.7 has an invalid write in readOHDRHeaderMessageDataLayout in hdf/dataobject.c. **CVE ID : CVE-2019-16093**	N/A	A-SYM-LIBM-230919/420
Out-of-bounds Read	07-09-2019	5	Symonics libmysofa 0.7 has an invalid read in readOHDRHeaderMessageDataLayout in hdf/dataobject.c.	N/A	A-SYM-LIBM-230919/421

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16094		
Out-of-bounds Read	07-09-2019	5	Symonics libmysofa 0.7 has an invalid read in getDimension in hrtf/reader.c. **CVE ID : CVE-2019-16095**	N/A	A-SYM-LIBM-230919/422
symphonyextensions					
rich_text_formatter					
Unrestricted Upload of File with Dangerous Type	05-09-2019	7.5	The Rich Text Formatter (Redactor) extension through v1.1.1 for Symphony CMS has an Unauthenticated arbitrary file upload vulnerability in content.fileupload.php and content.imageupload.php. **CVE ID : CVE-2019-13187**	N/A	A-SYM-RICH-230919/423
sysstat_project					
sysstat					
Integer Overflow or Wraparound	09-09-2019	4.3	sysstat before 12.1.6 has memory corruption due to an Integer Overflow in remap_struct() in sa_common.c. **CVE ID : CVE-2019-16167**	N/A	A-SYS-SYSS-230919/424
teammatesolutions					
Teammate+					
Cross-Site Request Forgery (CSRF)	09-09-2019	4.3	A Cross-Site Request Forgery (CSRF) vulnerability exists in TeamMate+ 21.0.0.0 that allows a remote attacker to modify application data (upload malicious/forged files on a TeamMate server, or replace existing uploaded files with malicious/forged files). The specific flaw exists within the handling of	N/A	A-TEA-TEAM-230919/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Upload/DomainObjectDocumentUpload.ashx requests because of failure to validate a CSRF token before handling a POST request. **CVE ID : CVE-2019-10253**		
Teamviewer					
teamviewer					
Insufficiently Protected Credentials	11-09-2019	7.2	An issue was discovered in TeamViewer 14.2.2558. Updating the product as a non-administrative user requires entering administrative credentials into the GUI. Subsequently, these credentials are processed in Teamviewer.exe, which allows any application running in the same non-administrative user context to intercept them in cleartext within process memory. By using this technique, a local attacker is able to obtain administrative credentials in order to elevate privileges. This vulnerability can be exploited by injecting code into Teamviewer.exe which intercepts calls to GetWindowTextW and logs the processed credentials. **CVE ID : CVE-2019-11769**	N/A	A-TEA-TEAM-230919/426
Telegram					
telegram					
Improper Input	11-09-2019	5	The "delete for" feature in Telegram before 5.11 on Android does not delete	N/A	A-TEL-TELE-230919/427

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			shared media files from the Telegram Images directory. In other words, there is a potentially misleading UI indication that a sender can remove a recipient's copy of a previously sent image (analogous to supported functionality in which a sender can remove a recipient's copy of a previously sent message). **CVE ID : CVE-2019-16248**		
tiktok					
tiktok					
Information Exposure	04-09-2019	3.3	The TikTok (formerly Musical.ly) application 12.2.0 for Android and iOS performs unencrypted transmission of images, videos, and likes. This allows an attacker to extract private sensitive information by sniffing network traffic. **CVE ID : CVE-2019-14319**	N/A	A-TIK-TIKT-230919/428
totaljs					
total.js_cms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-09-2019	6.5	An issue was discovered in Total.js CMS 12.0.0. An authenticated user with the Pages privilege can conduct a path traversal attack (../) to include .html files that are outside the permitted directory. Also, if a page contains a template directive, then the directive will be server side processed. Thus, if a user can control the	N/A	A-TOT-TOTA-230919/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			content of a .html file, then they can inject a payload with a malicious template directive to gain Remote Command Execution. The exploit will work only with the .html extension. **CVE ID : CVE-2019-15952**		
N/A	05-09-2019	6.5	An issue was discovered in Total.js CMS 12.0.0. An authenticated user with limited privileges can get access to a resource that they do not own by calling the associated API. The product correctly manages privileges only for the front-end resource path, not for API requests. This leads to vertical and horizontal privilege escalation. **CVE ID : CVE-2019-15953**	N/A	A-TOT-TOTA-230919/430
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-09-2019	9	An issue was discovered in Total.js CMS 12.0.0. An authenticated user with the widgets privilege can gain achieve Remote Command Execution (RCE) on the remote server by creating a malicious widget with a special tag containing JavaScript code that will be evaluated server side. In the process of evaluating the tag by the back-end, it is possible to escape the sandbox object by using the following payload: <script total>global.process.mainModule.require(child_process).e	N/A	A-TOT-TOTA-230919/431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			xec(RCE);</script> **CVE ID : CVE-2019-15954**		
Algorithmic Complexity	05-09-2019	4	An issue was discovered in Total.js CMS 12.0.0. A low privilege user can perform a simple transformation of a cookie to obtain the random values inside it. If an attacker can discover a session cookie owned by an admin, then it is possible to brute force it with O(n)=2n instead of O(n)=n^x complexity, and steal the admin password. **CVE ID : CVE-2019-15955**	N/A	A-TOT-TOTA-230919/432
Trendmicro					
deep_security_manager					
Improper Restriction of XML External Entity Reference ('XXE')	11-09-2019	4	Trend Micro Deep Security Manager (10.x, 11.x) and Vulnerability Protection (2.0) are vulnerable to a XML External Entity Attack. However, for the attack to be possible, the attacker must have root/admin access to a protected host which is authorized to communicate with the Deep Security Manager (DSM). **CVE ID : CVE-2019-9488**	N/A	A-TRE-DEEP-230919/433
vulnerability_protection					
Improper Restriction of XML External Entity Reference ('XXE')	11-09-2019	4	Trend Micro Deep Security Manager (10.x, 11.x) and Vulnerability Protection (2.0) are vulnerable to a XML External Entity Attack. However, for the attack to be possible, the attacker must	N/A	A-TRE-VULN-230919/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have root/admin access to a protected host which is authorized to communicate with the Deep Security Manager (DSM). **CVE ID : CVE-2019-9488**		
tri					
event_tickets					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-09-2019	6.5	CSV injection in the event-tickets (Event Tickets) plugin before 4.10.7.2 for WordPress exists via the "All Post> Ticketed > Attendees" Export Attendees feature. **CVE ID : CVE-2019-16120**	N/A	A-TRI-EVEN-230919/435
ttlock					
ttlock					
Improper Privilege Management	10-09-2019	3.3	TTLock devices do not properly block guest access in certain situations where the network connection to the cloud is unavailable. **CVE ID : CVE-2019-12942**	N/A	A-TTL-TTLO-230919/436
Weak Password Recovery Mechanism for Forgotten Password	10-09-2019	2.6	TTLock devices do not properly restrict password-reset attempts, leading to incorrect access control and disclosure of sensitive information about valid account names. **CVE ID : CVE-2019-12943**	N/A	A-TTL-TTLO-230919/437
ultra-prod					
wordpress_ultra_simple_paypal_shopping_cart					
Cross-Site Request	12-09-2019	6.8	Cross-site request forgery (CSRF) vulnerability in	N/A	A-ULT-WORD-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			WordPress Ultra Simple Paypal Shopping Cart v4.4 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID : CVE-2019-5992**		230919/438
userproplugin					
user_pro					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-09-2019	4.3	cosenary Instagram-PHP-API (aka Instagram PHP API V2), as used in the UserPro plugin through 4.9.32 for WordPress, has XSS via the example/success.php error_description parameter. **CVE ID : CVE-2019-14470**	N/A	A-USE-USER-230919/439
Varnish-cache					
varnish					
Improper Input Validation	03-09-2019	7.8	An issue was discovered in Varnish Cache before 6.0.4 LTS, and 6.1.x and 6.2.x before 6.2.1. An HTTP/1 parsing failure allows a remote attacker to trigger an assert by sending crafted HTTP/1 requests. The assert will cause an automatic restart with a clean cache, which makes it a Denial of Service attack. **CVE ID : CVE-2019-15892**	N/A	A-VAR-VARN-230919/440
W1.fi					
hostapd					
Improper Input	12-09-2019	3.3	hostapd before 2.10 and wpa_supplicant before 2.10	N/A	A-W1.-HOST-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			allow an incorrect indication of disconnection in certain situations because source address validation is mishandled. This is a denial of service that should have been prevented by PMF (aka management frame protection). The attacker must send a crafted 802.11 frame from a location that is within the 802.11 communications range. **CVE ID : CVE-2019-16275**		230919/441
wpa_supplicant					
Improper Input Validation	12-09-2019	3.3	hostapd before 2.10 and wpa_supplicant before 2.10 allow an incorrect indication of disconnection in certain situations because source address validation is mishandled. This is a denial of service that should have been prevented by PMF (aka management frame protection). The attacker must send a crafted 802.11 frame from a location that is within the 802.11 communications range. **CVE ID : CVE-2019-16275**	N/A	A-W1.-WPA_-230919/442
weaver					
eteams_oa					
Insufficient Session Expiration	08-09-2019	4	An issue was discovered in eteams OA v4.0.34. Because the session is not strictly checked, the account names and passwords of all employees in the company	N/A	A-WEA-ETEA-230919/443

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can be obtained by an ordinary account. Specifically, the attacker sends a jsessionid value for URIs under app/profile/summary/. **CVE ID : CVE-2019-16133**		
webcraftic					
woody_ad_snippets					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-09-2019	4.3	admin/includes/class.import.snippet.php in the "Woody ad snippets" plugin before 2.2.5 for WordPress allows unauthenticated options import, as demonstrated by storing an XSS payload for remote code execution. **CVE ID : CVE-2019-15858**	N/A	A-WEB-WOOD-230919/444
Wondercms					
wondercms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-09-2019	7.5	Directory traversal vulnerability in WonderCMS 2.6.0 and earlier allows remote attackers to delete arbitrary files via unspecified vectors. **CVE ID : CVE-2019-5956**	N/A	A-WON-WOND-230919/445
Wordpress					
wordpress					
Improper Neutralization of Input During Web Page Generation ('Cross-site	11-09-2019	4.3	WordPress before 5.2.3 allows XSS in media uploads because wp_ajax_upload_attachment is mishandled. **CVE ID : CVE-2019-16217**	N/A	A-WOR-WORD-230919/446

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	4.3	WordPress before 5.2.3 allows XSS in stored coments. **CVE ID : CVE-2019-16218**	N/A	A-WOR-WORD-230919/447
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	4.3	WordPress before 5.2.3 allows XSS in shortcode previews. **CVE ID : CVE-2019-16219**	N/A	A-WOR-WORD-230919/448
URL Redirection to Untrusted Site ('Open Redirect')	11-09-2019	5.8	In WordPress before 5.2.3, validation and sanitization of a URL in wp_validate_redirect in wp-includes/pluggable.php could lead to an open redirect. **CVE ID : CVE-2019-16220**	N/A	A-WOR-WORD-230919/449
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	4.3	WordPress before 5.2.3 allows reflected XSS in the dashboard. **CVE ID : CVE-2019-16221**	N/A	A-WOR-WORD-230919/450
Improper Neutralization of Input During Web Page Generation ('Cross-site	11-09-2019	4.3	WordPress before 5.2.3 has an issue with URL sanitization in wp_kses_bad_protocol_once in wp-includes/kses.php that can lead to cross-site scripting (XSS) attacks.	N/A	A-WOR-WORD-230919/451

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			**CVE ID : CVE-2019-16222**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	3.5	WordPress before 5.2.3 allows XSS in post previews by authenticated users. **CVE ID : CVE-2019-16223**	N/A	A-WOR-WORD-230919/452
wpaffiliatemanager					
affiliates_manager					
Cross-Site Request Forgery (CSRF)	03-09-2019	6.8	The affiliates-manager plugin before 2.6.6 for WordPress has CSRF. **CVE ID : CVE-2019-15868**	N/A	A-WPA-AFFI-230919/453
wpbrigade					
loginpress					
N/A	03-09-2019	4	The LoginPress plugin before 1.1.4 for WordPress has no capability check for updates to settings. **CVE ID : CVE-2019-15871**	N/A	A-WPB-LOGI-230919/454
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-09-2019	7.5	The LoginPress plugin before 1.1.4 for WordPress has SQL injection via an import of settings. **CVE ID : CVE-2019-15872**	N/A	A-WPB-LOGI-230919/455
youphptube					
youphptube					
Improper Privilege Management	08-09-2019	7.5	In YouPHPTube 7.4, the file install/checkConfiguration.php has no access control, which leads to everyone	N/A	A-YOU-YOUP-230919/456

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			being able to edit the configuration file, and insert malicious PHP code. **CVE ID : CVE-2019-16124**		
Operating System					
abus					
secvest_wireless_alarm_system_fuaa50000_firmware					
N/A	03-09-2019	5	An issue was discovered on ABUS Secvest FUAA50000 3.01.01 devices. Due to an insufficient implementation of jamming detection, an attacker is able to suppress correctly received RF messages sent between wireless peripheral components, e.g., wireless detectors or remote controls, and the ABUS Secvest alarm central. An attacker is able to perform a "reactive jamming" attack. The reactive jamming simply detects the start of a RF message sent by a component of the ABUS Secvest wireless alarm system, for instance a wireless motion detector (FUBW50000) or a remote control (FUBE50014 or FUBE50015), and overlays it with random data before the original RF message ends. Thereby, the receiver (alarm central) is not able to properly decode the original transmitted signal. This enables an attacker to suppress correctly received RF messages of the wireless	N/A	O-ABU-SECV-230919/457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			alarm system in an unauthorized manner, for instance status messages sent by a detector indicating an intrusion. **CVE ID : CVE-2019-14261**		
Canonical					
ubuntu_linux					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-09-2019	6.4	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share. **CVE ID : CVE-2019-10197**	N/A	O-CAN-UBUN-230919/458
dasanzhone					
znid_gpon_2426a_eu_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-09-2019	4.3	Multiple Cross-Site Scripting (XSS) issues in the web interface on DASAN Zhone ZNID GPON 2426A EU version S3.1.285 devices allow a remote attacker to execute arbitrary JavaScript via manipulation of an unsanitized GET parameter: /zhndnsdisplay.cmd (name), /wlsecrefresh.wl (wlWscCfgMethod, wl_wsc_reg). **CVE ID : CVE-2019-10677**	N/A	O-DAS-ZNID-230919/459
Debian					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
debian_linux					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-09-2019	6.4	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share. **CVE ID : CVE-2019-10197**	N/A	O-DEB-DEBI-230919/460
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-09-2019	10	Exim before 4.92.2 allows remote attackers to execute arbitrary code as root via a trailing backslash. **CVE ID : CVE-2019-15846**	N/A	O-DEB-DEBI-230919/461
Improper Input Validation	03-09-2019	7.8	An issue was discovered in Varnish Cache before 6.0.4 LTS, and 6.1.x and 6.2.x before 6.2.1. An HTTP/1 parsing failure allows a remote attacker to trigger an assert by sending crafted HTTP/1 requests. The assert will cause an automatic restart with a clean cache, which makes it a Denial of Service attack. **CVE ID : CVE-2019-15892**	N/A	O-DEB-DEBI-230919/462
Dlink					
dir-806_firmware					
Improper Control of	06-09-2019	10	D-Link DIR-806 devices allow remote attackers to execute	N/A	O-DLI-DIR--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			arbitrary shell commands via a trailing substring of an HTTP header that has "SOAPAction: http://purenetworks.com/HNAP1/GetDeviceSettings/" at the beginning. **CVE ID : CVE-2019-10891**		230919/463
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-09-2019	10	hnap_main in /htdocs/cgibin on D-link DIR-806 v1.0 devices has a stack-based buffer overflow via a long HTTP header that has "SOAPAction: http://purenetworks.com/HNAP1/GetDeviceSettings/" at the beginning. **CVE ID : CVE-2019-10892**	N/A	O-DLI-DIR--230919/464
dir-868l_firmware					
Improper Authentication	09-09-2019	7.5	SharePort Web Access on D-Link DIR-868L REVB through 2.03, DIR-885L REVA through 1.20, and DIR-895L REVA through 1.21 devices allows Authentication Bypass, as demonstrated by a direct request to folder_view.php or category_view.php. **CVE ID : CVE-2019-16190**	N/A	O-DLI-DIR--230919/465
dir-885l_firmware					
Improper Authentication	09-09-2019	7.5	SharePort Web Access on D-Link DIR-868L REVB through 2.03, DIR-885L REVA through 1.20, and DIR-895L REVA through 1.21 devices allows Authentication Bypass, as demonstrated by a direct request to	N/A	O-DLI-DIR--230919/466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			folder_view.php or category_view.php. **CVE ID : CVE-2019-16190**		
dir-895l_firmware					
Improper Authentication	09-09-2019	7.5	SharePort Web Access on D-Link DIR-868L REVB through 2.03, DIR-885L REVA through 1.20, and DIR-895L REVA through 1.21 devices allows Authentication Bypass, as demonstrated by a direct request to folder_view.php or category_view.php. **CVE ID : CVE-2019-16190**	N/A	O-DLI-DIR--230919/467
Fedoraproject					
fedora					
Improper Access Control	04-09-2019	2.1	In systemd 240, bus_open_system_watch_bind_with_description in shared/bus-util.c (as used by systemd-resolved to connect to the system D-Bus instance), calls sd_bus_set_trusted, which disables access controls for incoming D-Bus messages. An unprivileged user can exploit this by executing D-Bus methods that should be restricted to privileged users, in order to change the system's DNS resolver settings. **CVE ID : CVE-2019-15718**	N/A	O-FED-FEDO-230919/468
Google					
android					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	06-09-2019	7.8	In the Android kernel in VPN routing there is a possible information disclosure. This could lead to remote information disclosure by an adjacent network attacker with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9461**	N/A	O-GOO-ANDR-230919/469
Information Exposure	05-09-2019	2.1	In Google Assistant in Android 9, there is a possible permissions bypass that allows the Assistant to take a screenshot of apps with FLAG_SECURE. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-2103**	N/A	O-GOO-ANDR-230919/470
Out-of-bounds Write	05-09-2019	9.3	In ihevcd_ref_list of ihevcd_ref_list.c in Android 10, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2019-2108**	N/A	O-GOO-ANDR-230919/471
Double Free	05-09-2019	7.2	In GateKeeper::MintAuthToken of gatekeeper.cpp in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is possible memory	N/A	O-GOO-ANDR-230919/472

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-2115**		
N/A	05-09-2019	4.6	In execTransact of Binder.java in Android 7.1.1, 7.1.2, 8.0, 8.1, and 9, there is a possible local execution of arbitrary code in a privileged process due to a memory overwrite. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-2123**	N/A	O-GOO-ANDR-230919/473
Information Exposure	05-09-2019	2.1	In ComposeActivityEmailExternal of ComposeActivityEmailExternal.java in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is a possible way to silently attach files to an email due to a confused deputy. This could lead to local information disclosure. **CVE ID : CVE-2019-2124**	N/A	O-GOO-ANDR-230919/474
Use After Free	05-09-2019	7.2	In SensorManager::assertStateLocked of SensorManager.cpp in Android 7.1.1, 7.1.2, 8.0, 8.1, and 9, there is a possible use after free due to improper locking. This could	N/A	O-GOO-ANDR-230919/475

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-2174**		
N/A	05-09-2019	4.4	In checkAccess of SliceManagerService.java in Android 9, there is a possible permissions check bypass due to incorrect order of arguments. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2019-2175**	N/A	O-GOO-ANDR-230919/476
Out-of-bounds Write	05-09-2019	9.3	In ihevcd_parse_buffering_period_sei of ihevcd_parse_headers.c in Android 8.0, 8.1 and 9, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2019-2176**	N/A	O-GOO-ANDR-230919/477
N/A	05-09-2019	6.8	In isPreferred of HidProfile.java in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is a possible device type confusion due to a permissions bypass. This could lead to remote code	N/A	O-GOO-ANDR-230919/478

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution with no additional execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2019-2177**		
Out-of-bounds Write	05-09-2019	7.2	In rw_t4t_sm_read_ndef of rw_t4t in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the NFC service with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-2178**	N/A	O-GOO-ANDR-230919/479
Integer Overflow or Wraparound	05-09-2019	4.3	In NDEF_MsgValidate of ndef_utils in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2019-2179**	N/A	O-GOO-ANDR-230919/480
Improper Input Validation	05-09-2019	2.1	In ippSetValueTag of ipp.c in Android 8.0, 8.1 and 9, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure from the printer service with no additional execution privileges needed. User	N/A	O-GOO-ANDR-230919/481

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. **CVE ID : CVE-2019-2180**		
Integer Overflow or Wraparound	05-09-2019	6.9	In binder_transaction of binder.c in the Android kernel, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2019-2181**	N/A	O-GOO-ANDR-230919/482
N/A	06-09-2019	4.6	In the Android kernel in the kernel MMU code there is a possible execution path leaving some kernel text and rodata pages writable. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-2182**	N/A	O-GOO-ANDR-230919/483
Out-of-bounds Read	06-09-2019	2.1	In the Android kernel in the f2fs driver there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9245**	N/A	O-GOO-ANDR-230919/484
Out-of-bounds	06-09-2019	4.6	In the Android kernel in the FingerTipS touchscreen driver there is a possible out	N/A	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9248**		230919/485
Improper Input Validation	05-09-2019	7.2	In readArgumentList of zygote.java in Android 10, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9254**	N/A	O-GOO-ANDR-230919/486
Out-of-bounds Write	06-09-2019	4.6	In the Android kernel in unifi and r8180 WiFi drivers there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9270**	N/A	O-GOO-ANDR-230919/487
Use After Free	06-09-2019	4.4	In the Android kernel in the mnh driver there is a race condition due to insufficient locking. This could lead to a use-after-free which could lead to escalation of privilege with System execution privileges needed. User interaction is not needed for	N/A	O-GOO-ANDR-230919/488

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation. **CVE ID : CVE-2019-9271**		
Use After Free	06-09-2019	4.6	In the Android kernel in the synaptics_dsx_htc touchscreen driver there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9273**	N/A	O-GOO-ANDR-230919/489
Out-of-bounds Write	06-09-2019	4.6	In the Android kernel in the mnh driver there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9274**	N/A	O-GOO-ANDR-230919/490
Use After Free	06-09-2019	7.5	In the Android kernel in the mnh driver there is a use after free due to improper locking. This could lead to escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9275**	N/A	O-GOO-ANDR-230919/491
Use After Free	06-09-2019	4.6	In the Android kernel in the synaptics_dsx_htc touchscreen driver there is a possible out of bounds write due to a use after free. This could lead to a local escalation of privilege with	N/A	O-GOO-ANDR-230919/492

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9276**		
N/A	06-09-2019	7.2	In the Android kernel in sdcardfs there is a possible violation of the separation of data between profiles due to shared mapping of obb files. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2019-9345**	N/A	O-GOO-ANDR-230919/493
Out-of-bounds Write	06-09-2019	4.6	In the Android kernel in Bluetooth there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9426**	N/A	O-GOO-ANDR-230919/494
N/A	06-09-2019	4.6	In the Android kernel in the bootloader there is a possible secure boot bypass. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. **CVE ID : CVE-2019-9436**	N/A	O-GOO-ANDR-230919/495
Out-of-bounds Write	06-09-2019	4.6	In the Android kernel in the mnh driver there is a possible out of bounds write due to improper input validation. This could lead to	N/A	O-GOO-ANDR-230919/496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9441**		
Use After Free	06-09-2019	4.6	In the Android kernel in the mnh driver there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with System privileges required. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9442**	N/A	O-GOO-ANDR-230919/497
Out-of-bounds Write	06-09-2019	4.6	In the Android kernel in the vl53L0 driver there is a possible out of bounds write due to a permissions bypass. This could lead to local escalation of privilege due to a set_fs() call without restoring the previous limit with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9443**	N/A	O-GOO-ANDR-230919/498
Information Exposure	06-09-2019	2.1	In the Android kernel in sync debug fs driver there is a kernel pointer leak due to the usage of printf with %p. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9444**	N/A	O-GOO-ANDR-230919/499
Out-of-	06-09-2019	2.1	In the Android kernel in F2FS driver there is a possible out	N/A	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			of bounds read due to a missing bounds check. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9445**		230919/500
Out-of-bounds Write	06-09-2019	4.6	In the Android kernel in the FingerTipS touchscreen driver there is a possible out of bounds write due to improper input validation. This could lead to a local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9446**	N/A	O-GOO-ANDR-230919/501
Use After Free	06-09-2019	4.6	In the Android kernel in the FingerTipS touchscreen driver there is a possible use-after-free due to improper locking. This could lead to a local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9447**	N/A	O-GOO-ANDR-230919/502
Out-of-bounds Write	06-09-2019	4.6	In the Android kernel in the FingerTipS touchscreen driver there is a possible out of bounds write due to a missing bounds check. This could lead to a local escalation of privilege with System execution privileges needed. User interaction is	N/A	O-GOO-ANDR-230919/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. **CVE ID : CVE-2019-9448**		
Out-of-bounds Read	06-09-2019	2.1	In the Android kernel in FingerTipS touchscreen driver there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9449**	N/A	O-GOO-ANDR-230919/504
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-09-2019	4.4	In the Android kernel in the FingerTipS touchscreen driver there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9450**	N/A	O-GOO-ANDR-230919/505
Out-of-bounds Write	06-09-2019	4.6	In the Android kernel in the touchscreen driver there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9451**	N/A	O-GOO-ANDR-230919/506
Out-of-bounds Read	06-09-2019	2.1	In the Android kernel in SEC_TS touch driver there is a possible out of bounds read due to a missing bounds check. This could lead to local	N/A	O-GOO-ANDR-230919/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9452**		
Improper Input Validation	06-09-2019	2.1	In the Android kernel in F2FS touch driver there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9453**	N/A	O-GOO-ANDR-230919/508
Out-of-bounds Write	06-09-2019	4.6	In the Android kernel in i2c driver there is a possible out of bounds write due to memory corruption. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9454**	N/A	O-GOO-ANDR-230919/509
Information Exposure	06-09-2019	2.1	In the Android kernel in the video driver there is a kernel pointer leak due to a WARN_ON statement. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9455**	N/A	O-GOO-ANDR-230919/510
Out-of-bounds	06-09-2019	4.6	In the Android kernel in Pixel C USB monitor driver there is a possible OOB write due to a	N/A	O-GOO-ANDR-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9456**		230919/511
Integer Overflow or Wraparound	06-09-2019	4.6	In the Android kernel in ELF file loading there is possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9457**	N/A	O-GOO-ANDR-230919/512
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-09-2019	4.4	In the Android kernel in the video driver there is a use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE ID : CVE-2019-9458**	N/A	O-GOO-ANDR-230919/513
hanwha-security					
srn-472s_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-09-2019	7.8	An issue was discovered in NVR WebViewer on Hanwah Techwin SRN-472s 1.07_190502 devices, and other SRN-x devices before 2019-05-03. A system crash and reboot can be achieved by submitting a long username in excess of 117 characters. The username	N/A	O-HAN-SRN--230919/514

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			triggers a buffer overflow in the main process controlling operation of the DVR system, rendering services unavailable during the reboot operation. A repeated attack affects availability as long as the attacker has network access to the device. **CVE ID : CVE-2019-12223**		
Linux					
linux_kernel					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-09-2019	7.5	A backporting error was discovered in the Linux stable/longterm kernel 4.4.x through 4.4.190, 4.9.x through 4.9.190, 4.14.x through 4.14.141, 4.19.x through 4.19.69, and 5.2.x through 5.2.11. Misuse of the upstream "x86/ptrace: Fix possible spectre-v1 in ptrace_get_debugreg()" commit reintroduced the Spectre vulnerability that it aimed to eliminate. This occurred because the backport process depends on cherry picking specific commits, and because two (correctly ordered) code lines were swapped. **CVE ID : CVE-2019-15902**	N/A	O-LIN-LINU-230919/515
Improper Restriction of Operations within the Bounds of a	04-09-2019	7.8	An issue was discovered in the Linux kernel before 5.0.1. There is a memory leak in register_queue_kobjects() in net/core/net-sysfs.c, which will cause denial of service.	N/A	O-LIN-LINU-230919/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			**CVE ID : CVE-2019-15916**		
Use After Free	04-09-2019	7.2	An issue was discovered in the Linux kernel before 5.0.5. There is a use-after-free issue when hci_uart_register_dev() fails in hci_uart_set_proto() in drivers/bluetooth/hci_ldisc.c. **CVE ID : CVE-2019-15917**	N/A	O-LIN-LINU-230919/517
Out-of-bounds Read	04-09-2019	7.2	An issue was discovered in the Linux kernel before 5.0.10. SMB2_negotiate in fs/cifs/smb2pdu.c has an out-of-bounds read because data structures are incompletely updated after a change from smb30 to smb21. **CVE ID : CVE-2019-15918**	N/A	O-LIN-LINU-230919/518
Use After Free	04-09-2019	7.2	An issue was discovered in the Linux kernel before 5.0.10. SMB2_write in fs/cifs/smb2pdu.c has a use-after-free. **CVE ID : CVE-2019-15919**	N/A	O-LIN-LINU-230919/519
Use After Free	04-09-2019	7.2	An issue was discovered in the Linux kernel before 5.0.10. SMB2_read in fs/cifs/smb2pdu.c has a use-after-free. NOTE: this was not fixed correctly in 5.0.10; see the 5.0.11 ChangeLog, which documents a memory leak. **CVE ID : CVE-2019-15920**	N/A	O-LIN-LINU-230919/520
N/A	04-09-2019	4.6	An issue was discovered in the Linux kernel before 5.0.6. There is a memory leak issue when idr_alloc() fails in	N/A	O-LIN-LINU-230919/521

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			genl_register_family() in net/netlink/genetlink.c. **CVE ID : CVE-2019-15921**		
NULL Pointer Dereference	04-09-2019	4.9	An issue was discovered in the Linux kernel before 5.0.9. There is a NULL pointer dereference for a pf data structure if alloc_disk fails in drivers/block/paride/pf.c. **CVE ID : CVE-2019-15922**	N/A	O-LIN-LINU-230919/522
NULL Pointer Dereference	04-09-2019	4.9	An issue was discovered in the Linux kernel before 5.0.9. There is a NULL pointer dereference for a cd data structure if alloc_disk fails in drivers/block/paride/pf.c. **CVE ID : CVE-2019-15923**	N/A	O-LIN-LINU-230919/523
NULL Pointer Dereference	04-09-2019	4.9	An issue was discovered in the Linux kernel before 5.0.11. fm10k_init_module in drivers/net/ethernet/intel/fm10k/fm10k_main.c has a NULL pointer dereference because there is no -ENOMEM upon an alloc_workqueue failure. **CVE ID : CVE-2019-15924**	N/A	O-LIN-LINU-230919/524
Out-of-bounds Read	04-09-2019	7.2	An issue was discovered in the Linux kernel before 5.2.3. An out of bounds access exists in the function hclge_tm_schd_mode_vnet_base_cfg in the file drivers/net/ethernet/hisilicon/hns3/hns3pf/hclge_tm.c. **CVE ID : CVE-2019-15925**	N/A	O-LIN-LINU-230919/525
Out-of-bounds Read	04-09-2019	9.4	An issue was discovered in the Linux kernel before 5.2.3.	N/A	O-LIN-LINU-230919/526

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Out of bounds access exists in the functions ath6kl_wmi_pstream_timeout_event_rx and ath6kl_wmi_cac_event_rx in the file drivers/net/wireless/ath/ath6kl/wmi.c. **CVE ID : CVE-2019-15926**		
Out-of-bounds Read	04-09-2019	7.2	An issue was discovered in the Linux kernel before 4.20.2. An out-of-bounds access exists in the function build_audio_procunit in the file sound/usb/mixer.c. **CVE ID : CVE-2019-15927**	N/A	O-LIN-LINU-230919/527
NULL Pointer Dereference	06-09-2019	7.5	An issue was discovered in the Linux kernel through 5.2.13. nbd_genl_status in drivers/block/nbd.c does not check the nla_nest_start_noflag return value. **CVE ID : CVE-2019-16089**	N/A	O-LIN-LINU-230919/528
NULL Pointer Dereference	11-09-2019	7.8	drivers/gpu/drm/amd/amdkfd/kfd_interrupt.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference. **CVE ID : CVE-2019-16229**	N/A	O-LIN-LINU-230919/529
NULL Pointer Dereference	11-09-2019	7.8	drivers/gpu/drm/radeon/radeon_display.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference. **CVE ID : CVE-2019-16230**	N/A	O-LIN-LINU-230919/530

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	11-09-2019	7.8	drivers/net/fjes/fjes_main.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference. **CVE ID : CVE-2019-16231**	N/A	O-LIN-LINU-230919/531
NULL Pointer Dereference	11-09-2019	7.8	drivers/net/wireless/marvell/libertas/if_sdio.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference. **CVE ID : CVE-2019-16232**	N/A	O-LIN-LINU-230919/532
NULL Pointer Dereference	11-09-2019	7.8	drivers/scsi/qla2xxx/qla_os.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference. **CVE ID : CVE-2019-16233**	N/A	O-LIN-LINU-230919/533
NULL Pointer Dereference	11-09-2019	7.8	drivers/net/wireless/intel/iwlwifi/pcie/trans.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference. **CVE ID : CVE-2019-16234**	N/A	O-LIN-LINU-230919/534
Microsoft					
azure_devops_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	3.5	A Cross-site Scripting (XSS) vulnerability exists when Team Foundation Server does not properly sanitize user provided input, aka 'Team Foundation Server Cross-site Scripting Vulnerability'.	N/A	O-MIC-AZUR-230919/535

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1305		
Improper Input Validation	11-09-2019	7.5	A remote code execution vulnerability exists when Azure DevOps Server (ADO) and Team Foundation Server (TFS) fail to validate input properly, aka 'Azure DevOps and Team Foundation Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1306**	N/A	O-MIC-AZUR-230919/536
windows_10					
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0788, CVE-2019-1290, CVE-2019-1291. **CVE ID : CVE-2019-0787**	N/A	O-MIC-WIND-230919/537
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-1290, CVE-2019-1291. **CVE ID : CVE-2019-0788**	N/A	O-MIC-WIND-230919/538
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing	N/A	O-MIC-WIND-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073. **CVE ID : CVE-2019-1125**		230919/539
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249. **CVE ID : CVE-2019-1250**	N/A	O-MIC-WIND-230919/540
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1244, CVE-2019-1245. **CVE ID : CVE-2019-1251**	N/A	O-MIC-WIND-230919/541
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information	N/A	O-MIC-WIND-230919/542

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1286. **CVE ID : CVE-2019-1252**		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1215, CVE-2019-1278, CVE-2019-1303. **CVE ID : CVE-2019-1253**	N/A	O-MIC-WIND-230919/543
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1280**	N/A	O-MIC-WIND-230919/544
Improper Input Validation	11-09-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of	N/A	O-MIC-WIND-230919/545

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Vulnerability'. **CVE ID : CVE-2019-0928**		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1214**	N/A	O-MIC-WIND-230919/546
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in the way that ws2ifsl.sys (Winsock) handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1253, CVE-2019-1278, CVE-2019-1303. **CVE ID : CVE-2019-1215**	N/A	O-MIC-WIND-230919/547
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1216**	N/A	O-MIC-WIND-230919/548
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows Transaction Manager improperly handles objects in memory, aka 'Windows Transaction Manager Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-230919/549

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1219		
Improper Privilege Management	11-09-2019	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly impersonates certain file operations, aka 'Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1232**	N/A	O-MIC-WIND-230919/550
Improper Input Validation	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server process does not validate the source of input or commands it receives, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1235**	N/A	O-MIC-WIND-230919/551
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1208. **CVE ID : CVE-2019-1236**	N/A	O-MIC-WIND-230919/552
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-230919/553

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1240**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1241**	N/A	O-MIC-WIND-230919/554
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1242**	N/A	O-MIC-WIND-230919/555
Improper Restriction	11-09-2019	9.3	A remote code execution vulnerability exists when the	N/A	O-MIC-WIND-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1243**		230919/556
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1245, CVE-2019-1251. **CVE ID : CVE-2019-1244**	N/A	O-MIC-WIND-230919/557
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1244, CVE-2019-1251. **CVE ID : CVE-2019-1245**	N/A	O-MIC-WIND-230919/558
Improper Restriction of Operations within the Bounds of a	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote	N/A	O-MIC-WIND-230919/559

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1246**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1247**	N/A	O-MIC-WIND-230919/560
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1248**	N/A	O-MIC-WIND-230919/561

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1250. **CVE ID : CVE-2019-1249**	N/A	O-MIC-WIND-230919/562
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when Windows Hyper-V writes uninitialized memory to disk, aka 'Windows Hyper-V Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1254**	N/A	O-MIC-WIND-230919/563
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1285. **CVE ID : CVE-2019-1256**	N/A	O-MIC-WIND-230919/564
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Compatibility Appraiser where a configuration file, with local privileges, is vulnerable to	N/A	O-MIC-WIND-230919/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			symbolic link and hard link attacks, aka 'Microsoft Compatibility Appraiser Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1267**		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists when Winlogon does not properly handle file path information, aka 'Winlogon Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1268**	N/A	O-MIC-WIND-230919/566
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1272. **CVE ID : CVE-2019-1269**	N/A	O-MIC-WIND-230919/567
Improper Privilege Management	11-09-2019	3.6	An elevation of privilege vulnerability exists in Windows store installer where WindowsApps directory is vulnerable to symbolic link attack, aka 'Microsoft Windows Store Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1270**	N/A	O-MIC-WIND-230919/568
Improper Privilege	11-09-2019	7.2	An elevation of privilege exists in hdAudio.sys which	N/A	O-MIC-WIND-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			may lead to an out of band write, aka 'Windows Media Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1271**		230919/569
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1269. **CVE ID : CVE-2019-1272**	N/A	O-MIC-WIND-230919/570
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when Active Directory Federation Services (ADFS) does not properly sanitize certain error messages, aka 'Active Directory Federation Services XSS Vulnerability'. **CVE ID : CVE-2019-1273**	N/A	O-MIC-WIND-230919/571
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1274**	N/A	O-MIC-WIND-230919/572
Improper Privilege	11-09-2019	4.6	An elevation of privilege vulnerability exists in Windows Audio Service	N/A	O-MIC-WIND-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			when a malformed parameter is processed, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1277**		230919/573
Improper Privilege Management	11-09-2019	4.6	An elevation of privilege vulnerability exists in the way that the unistore.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1215, CVE-2019-1253, CVE-2019-1303. **CVE ID : CVE-2019-1278**	N/A	O-MIC-WIND-230919/574
Information Exposure	11-09-2019	2.1	An information disclosure exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle sandbox checks, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1282**	N/A	O-MIC-WIND-230919/575
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1256. **CVE ID : CVE-2019-1285**	N/A	O-MIC-WIND-230919/576
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component	N/A	O-MIC-WIND-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1252. **CVE ID : CVE-2019-1286**		230919/577
Improper Input Validation	11-09-2019	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connectivity Assistant handles objects in memory, aka 'Windows Network Connectivity Assistant Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1287**	N/A	O-MIC-WIND-230919/578
Improper Privilege Management	11-09-2019	3.6	An elevation of privilege vulnerability exists when the Windows Update Delivery Optimization does not properly enforce file share permissions, aka 'Windows Update Delivery Optimization Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1289**	N/A	O-MIC-WIND-230919/579
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1291. **CVE ID : CVE-2019-1290**	N/A	O-MIC-WIND-230919/580

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1290. **CVE ID : CVE-2019-1291**	N/A	O-MIC-WIND-230919/581
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	6.8	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-1292**	N/A	O-MIC-WIND-230919/582
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists in Windows when the Windows SMB Client kernel-mode driver fails to properly handle objects in memory, aka 'Windows SMB Client Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1293**	N/A	O-MIC-WIND-230919/583
Improper Input Validation	11-09-2019	2.1	A security feature bypass exists when Windows Secure Boot improperly restricts access to debugging functionality, aka 'Windows Secure Boot Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1294**	N/A	O-MIC-WIND-230919/584
Improper	11-09-2019	7.2	An elevation of privilege	N/A	O-MIC-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists when the Windows AppX Deployment Server improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1215, CVE-2019-1253, CVE-2019-1278. **CVE ID : CVE-2019-1303**		WIND-230919/585
windows_7					
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0788, CVE-2019-1290, CVE-2019-1291. **CVE ID : CVE-2019-0787**	N/A	O-MIC-WIND-230919/586
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073. **CVE ID : CVE-2019-1125**	N/A	O-MIC-WIND-230919/587
Improper	11-09-2019	9.3	A remote code execution	N/A	O-MIC-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249. **CVE ID : CVE-2019-1250**		WIND-230919/588
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1286. **CVE ID : CVE-2019-1252**	N/A	O-MIC-WIND-230919/589
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1280**	N/A	O-MIC-WIND-230919/590
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when the Windows Common Log File	N/A	O-MIC-WIND-230919/591

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1214**		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in the way that ws2ifsl.sys (Winsock) handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1253, CVE-2019-1278, CVE-2019-1303. **CVE ID : CVE-2019-1215**	N/A	O-MIC-WIND-230919/592
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1216**	N/A	O-MIC-WIND-230919/593
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows Transaction Manager improperly handles objects in memory, aka 'Windows Transaction Manager Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1219**	N/A	O-MIC-WIND-230919/594
Improper Input Validation	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server process does not	N/A	O-MIC-WIND-230919/595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validate the source of input or commands it receives, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1235**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1208. **CVE ID : CVE-2019-1236**	N/A	O-MIC-WIND-230919/596
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1240**	N/A	O-MIC-WIND-230919/597
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240,	N/A	O-MIC-WIND-230919/598

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1242**	N/A	O-MIC-WIND-230919/599
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1243**	N/A	O-MIC-WIND-230919/600
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly	N/A	O-MIC-WIND-230919/601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1245, CVE-2019-1251. **CVE ID : CVE-2019-1244**		
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1244, CVE-2019-1251. **CVE ID : CVE-2019-1245**	N/A	O-MIC-WIND-230919/602
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1246**	N/A	O-MIC-WIND-230919/603
Improper Restriction of Operations within the Bounds of a Memory	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution	N/A	O-MIC-WIND-230919/604

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1247**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1248**	N/A	O-MIC-WIND-230919/605
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1250. **CVE ID : CVE-2019-1249**	N/A	O-MIC-WIND-230919/606
Improper	11-09-2019	7.2	An elevation of privilege	N/A	O-MIC-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1285. **CVE ID : CVE-2019-1256**		WIND-230919/607
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Compatibility Appraiser where a configuration file, with local privileges, is vulnerable to symbolic link and hard link attacks, aka 'Microsoft Compatibility Appraiser Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1267**	N/A	O-MIC-WIND-230919/608
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists when Winlogon does not properly handle file path information, aka 'Winlogon Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1268**	N/A	O-MIC-WIND-230919/609
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists in hdAudio.sys which may lead to an out of band write, aka 'Windows Media Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1271**	N/A	O-MIC-WIND-230919/610
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory	N/A	O-MIC-WIND-230919/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			address, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1274**		
Information Exposure	11-09-2019	2.1	An information disclosure exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle sandbox checks, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1282**	N/A	O-MIC-WIND-230919/612
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1283**	N/A	O-MIC-WIND-230919/613
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1284**	N/A	O-MIC-WIND-230919/614
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-230919/615

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-1256. **CVE ID : CVE-2019-1285**		
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1252. **CVE ID : CVE-2019-1286**	N/A	O-MIC-WIND-230919/616
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1291. **CVE ID : CVE-2019-1290**	N/A	O-MIC-WIND-230919/617
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1290. **CVE ID : CVE-2019-1291**	N/A	O-MIC-WIND-230919/618
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists in Windows when the Windows	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMB Client kernel-mode driver fails to properly handle objects in memory, aka 'Windows SMB Client Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1293**		230919/619
windows_8.1					
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0788, CVE-2019-1290, CVE-2019-1291. **CVE ID : CVE-2019-0787**	N/A	O-MIC-WIND-230919/620
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-1290, CVE-2019-1291. **CVE ID : CVE-2019-0788**	N/A	O-MIC-WIND-230919/621
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure	N/A	O-MIC-WIND-230919/622

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073. **CVE ID : CVE-2019-1125**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249. **CVE ID : CVE-2019-1250**	N/A	O-MIC-WIND-230919/623
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1286. **CVE ID : CVE-2019-1252**	N/A	O-MIC-WIND-230919/624
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code	N/A	O-MIC-WIND-230919/625

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability'. **CVE ID : CVE-2019-1280**		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1214**	N/A	O-MIC-WIND-230919/626
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in the way that ws2ifsl.sys (Winsock) handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1253, CVE-2019-1278, CVE-2019-1303. **CVE ID : CVE-2019-1215**	N/A	O-MIC-WIND-230919/627
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1216**	N/A	O-MIC-WIND-230919/628
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows Transaction Manager improperly handles objects in memory, aka 'Windows Transaction Manager Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-230919/629

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1219		
Improper Input Validation	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server process does not validate the source of input or commands it receives, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1235**	N/A	O-MIC-WIND-230919/630
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1208. **CVE ID : CVE-2019-1236**	N/A	O-MIC-WIND-230919/631
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1240**	N/A	O-MIC-WIND-230919/632
Improper Restriction of	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database	N/A	O-MIC-WIND-230919/633

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1242**	N/A	O-MIC-WIND-230919/634
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-	N/A	O-MIC-WIND-230919/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1250. **CVE ID : CVE-2019-1243**		
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1245, CVE-2019-1251. **CVE ID : CVE-2019-1244**	N/A	O-MIC-WIND-230919/636
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1244, CVE-2019-1251. **CVE ID : CVE-2019-1245**	N/A	O-MIC-WIND-230919/637
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1246**	N/A	O-MIC-WIND-230919/638
Improper Restriction	11-09-2019	9.3	A remote code execution vulnerability exists when the	N/A	O-MIC-WIND-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1247**		230919/639
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1248**	N/A	O-MIC-WIND-230919/640
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247,	N/A	O-MIC-WIND-230919/641

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		🟥	CVE-2019-1248, CVE-2019-1250. **CVE ID : CVE-2019-1249**		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1285. **CVE ID : CVE-2019-1256**	N/A	O-MIC-WIND-230919/642
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Compatibility Appraiser where a configuration file, with local privileges, is vulnerable to symbolic link and hard link attacks, aka 'Microsoft Compatibility Appraiser Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1267**	N/A	O-MIC-WIND-230919/643
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists when Winlogon does not properly handle file path information, aka 'Winlogon Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1268**	N/A	O-MIC-WIND-230919/644
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability	N/A	O-MIC-WIND-230919/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1272. **CVE ID : CVE-2019-1269**		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists in hdAudio.sys which may lead to an out of band write, aka 'Windows Media Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1271**	N/A	O-MIC-WIND-230919/646
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1274**	N/A	O-MIC-WIND-230919/647
Information Exposure	11-09-2019	2.1	An information disclosure exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle sandbox checks, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1282**	N/A	O-MIC-WIND-230919/648
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-230919/649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2019-1256. **CVE ID : CVE-2019-1285**		
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1252. **CVE ID : CVE-2019-1286**	N/A	O-MIC-WIND-230919/650
Improper Input Validation	11-09-2019	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connectivity Assistant handles objects in memory, aka 'Windows Network Connectivity Assistant Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1287**	N/A	O-MIC-WIND-230919/651
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1291. **CVE ID : CVE-2019-1290**	N/A	O-MIC-WIND-230919/652
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects	N/A	O-MIC-WIND-230919/653

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1290. **CVE ID : CVE-2019-1291**		
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists in Windows when the Windows SMB Client kernel-mode driver fails to properly handle objects in memory, aka 'Windows SMB Client Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1293**	N/A	O-MIC-WIND-230919/654
windows_rt_8.1					
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0788, CVE-2019-1290, CVE-2019-1291. **CVE ID : CVE-2019-0787**	N/A	O-MIC-WIND-230919/655
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-230919/656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2019-0787, CVE-2019-1290, CVE-2019-1291. **CVE ID : CVE-2019-0788**		
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073. **CVE ID : CVE-2019-1125**	N/A	O-MIC-WIND-230919/657
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249. **CVE ID : CVE-2019-1250**	N/A	O-MIC-WIND-230919/658
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1286.	N/A	O-MIC-WIND-230919/659

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1252		
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1280**	N/A	O-MIC-WIND-230919/660
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1214**	N/A	O-MIC-WIND-230919/661
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in the way that ws2ifsl.sys (Winsock) handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1253, CVE-2019-1278, CVE-2019-1303. **CVE ID : CVE-2019-1215**	N/A	O-MIC-WIND-230919/662
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Information	N/A	O-MIC-WIND-230919/663

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. **CVE ID : CVE-2019-1216**		
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows Transaction Manager improperly handles objects in memory, aka 'Windows Transaction Manager Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1219**	N/A	O-MIC-WIND-230919/664
Improper Input Validation	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server process does not validate the source of input or commands it receives, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1235**	N/A	O-MIC-WIND-230919/665
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1208. **CVE ID : CVE-2019-1236**	N/A	O-MIC-WIND-230919/666
Improper Restriction of Operations within the Bounds of a Memory	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-230919/667

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			unique from CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1240**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1241**	N/A	O-MIC-WIND-230919/668
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1242**	N/A	O-MIC-WIND-230919/669
Improper Restriction	11-09-2019	9.3	A remote code execution vulnerability exists when the	N/A	O-MIC-WIND-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1243**		230919/670
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1245, CVE-2019-1251. **CVE ID : CVE-2019-1244**	N/A	O-MIC-WIND-230919/671
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1244, CVE-2019-1251. **CVE ID : CVE-2019-1245**	N/A	O-MIC-WIND-230919/672
Improper Restriction of Operations within the Bounds of a	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote	N/A	O-MIC-WIND-230919/673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1246**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1247**	N/A	O-MIC-WIND-230919/674
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1248**	N/A	O-MIC-WIND-230919/675

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1250. **CVE ID : CVE-2019-1249**	N/A	O-MIC-WIND-230919/676
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1285. **CVE ID : CVE-2019-1256**	N/A	O-MIC-WIND-230919/677
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists when Winlogon does not properly handle file path information, aka 'Winlogon Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1268**	N/A	O-MIC-WIND-230919/678
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability	N/A	O-MIC-WIND-230919/679

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1272. **CVE ID : CVE-2019-1269**		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists in hdAudio.sys which may lead to an out of band write, aka 'Windows Media Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1271**	N/A	O-MIC-WIND-230919/680
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1274**	N/A	O-MIC-WIND-230919/681
Information Exposure	11-09-2019	2.1	An information disclosure exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle sandbox checks, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1282**	N/A	O-MIC-WIND-230919/682
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-230919/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2019-1256. **CVE ID : CVE-2019-1285**		
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1252. **CVE ID : CVE-2019-1286**	N/A	O-MIC-WIND-230919/684
Improper Input Validation	11-09-2019	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connectivity Assistant handles objects in memory, aka 'Windows Network Connectivity Assistant Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1287**	N/A	O-MIC-WIND-230919/685
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1291. **CVE ID : CVE-2019-1290**	N/A	O-MIC-WIND-230919/686
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects	N/A	O-MIC-WIND-230919/687

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1290. **CVE ID : CVE-2019-1291**		
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists in Windows when the Windows SMB Client kernel-mode driver fails to properly handle objects in memory, aka 'Windows SMB Client Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1293**	N/A	O-MIC-WIND-230919/688
windows_server_2008					
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073. **CVE ID : CVE-2019-1125**	N/A	O-MIC-WIND-230919/689
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240,	N/A	O-MIC-WIND-230919/690

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249. **CVE ID : CVE-2019-1250**		
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1286. **CVE ID : CVE-2019-1252**	N/A	O-MIC-WIND-230919/691
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1280**	N/A	O-MIC-WIND-230919/692
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1214**	N/A	O-MIC-WIND-230919/693

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in the way that ws2ifsl.sys (Winsock) handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1253, CVE-2019-1278, CVE-2019-1303. **CVE ID : CVE-2019-1215**	N/A	O-MIC-WIND-230919/694
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1216**	N/A	O-MIC-WIND-230919/695
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows Transaction Manager improperly handles objects in memory, aka 'Windows Transaction Manager Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1219**	N/A	O-MIC-WIND-230919/696
Improper Input Validation	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server process does not validate the source of input or commands it receives, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1235**	N/A	O-MIC-WIND-230919/697

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1208. **CVE ID : CVE-2019-1236**	N/A	O-MIC-WIND-230919/698
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1240**	N/A	O-MIC-WIND-230919/699
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1241**	N/A	O-MIC-WIND-230919/700

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1242**	N/A	O-MIC-WIND-230919/701
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1243**	N/A	O-MIC-WIND-230919/702
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1245, CVE-2019-1251.	N/A	O-MIC-WIND-230919/703

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1244		
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1244, CVE-2019-1251. **CVE ID : CVE-2019-1245**	N/A	O-MIC-WIND-230919/704
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1246**	N/A	O-MIC-WIND-230919/705
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1248, CVE-2019-1249, CVE-2019-	N/A	O-MIC-WIND-230919/706

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1250. **CVE ID : CVE-2019-1247**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1248**	N/A	O-MIC-WIND-230919/707
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1250. **CVE ID : CVE-2019-1249**	N/A	O-MIC-WIND-230919/708
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-230919/709

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2019-1285. **CVE ID : CVE-2019-1256**		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Compatibility Appraiser where a configuration file, with local privileges, is vulnerable to symbolic link and hard link attacks, aka 'Microsoft Compatibility Appraiser Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1267**	N/A	O-MIC-WIND-230919/710
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists when Winlogon does not properly handle file path information, aka 'Winlogon Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1268**	N/A	O-MIC-WIND-230919/711
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists in hdAudio.sys which may lead to an out of band write, aka 'Windows Media Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1271**	N/A	O-MIC-WIND-230919/712
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1274**	N/A	O-MIC-WIND-230919/713
Information	11-09-2019	2.1	An information disclosure	N/A	O-MIC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle sandbox checks, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1282**		WIND-230919/714
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1283**	N/A	O-MIC-WIND-230919/715
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1284**	N/A	O-MIC-WIND-230919/716
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1256. **CVE ID : CVE-2019-1285**	N/A	O-MIC-WIND-230919/717
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component	N/A	O-MIC-WIND-230919/718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1252. **CVE ID : CVE-2019-1286**		
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1291. **CVE ID : CVE-2019-1290**	N/A	O-MIC-WIND-230919/719
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1290. **CVE ID : CVE-2019-1291**	N/A	O-MIC-WIND-230919/720
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists in Windows when the Windows SMB Client kernel-mode driver fails to properly handle objects in memory, aka 'Windows SMB Client Driver Information	N/A	O-MIC-WIND-230919/721

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. **CVE ID : CVE-2019-1293**		
windows_server_2012					
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073. **CVE ID : CVE-2019-1125**	N/A	O-MIC-WIND-230919/722
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249. **CVE ID : CVE-2019-1250**	N/A	O-MIC-WIND-230919/723
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1286.	N/A	O-MIC-WIND-230919/724

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1252		
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1280**	N/A	O-MIC-WIND-230919/725
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1214**	N/A	O-MIC-WIND-230919/726
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in the way that ws2ifsl.sys (Winsock) handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1253, CVE-2019-1278, CVE-2019-1303. **CVE ID : CVE-2019-1215**	N/A	O-MIC-WIND-230919/727
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Information	N/A	O-MIC-WIND-230919/728

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. **CVE ID : CVE-2019-1216**		
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows Transaction Manager improperly handles objects in memory, aka 'Windows Transaction Manager Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1219**	N/A	O-MIC-WIND-230919/729
Improper Input Validation	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server process does not validate the source of input or commands it receives, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1235**	N/A	O-MIC-WIND-230919/730
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1208. **CVE ID : CVE-2019-1236**	N/A	O-MIC-WIND-230919/731
Improper Restriction of Operations within the Bounds of a Memory	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-230919/732

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			unique from CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1240**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1241**	N/A	O-MIC-WIND-230919/733
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1242**	N/A	O-MIC-WIND-230919/734
Improper Restriction	11-09-2019	9.3	A remote code execution vulnerability exists when the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1243**		230919/735
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1245, CVE-2019-1251. **CVE ID : CVE-2019-1244**	N/A	O-MIC-WIND-230919/736
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1244, CVE-2019-1251. **CVE ID : CVE-2019-1245**	N/A	O-MIC-WIND-230919/737
Improper Restriction of Operations within the Bounds of a	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote	N/A	O-MIC-WIND-230919/738

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1246**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1247**	N/A	O-MIC-WIND-230919/739
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1248**	N/A	O-MIC-WIND-230919/740

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1250. **CVE ID : CVE-2019-1249**	N/A	O-MIC-WIND-230919/741
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1285. **CVE ID : CVE-2019-1256**	N/A	O-MIC-WIND-230919/742
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Compatibility Appraiser where a configuration file, with local privileges, is vulnerable to symbolic link and hard link attacks, aka 'Microsoft Compatibility Appraiser Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1267**	N/A	O-MIC-WIND-230919/743
Improper Privilege	11-09-2019	7.2	An elevation of privilege exists when Winlogon does	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			not properly handle file path information, aka 'Winlogon Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1268**		230919/744
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1272. **CVE ID : CVE-2019-1269**	N/A	O-MIC-WIND-230919/745
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists in hdAudio.sys which may lead to an out of band write, aka 'Windows Media Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1271**	N/A	O-MIC-WIND-230919/746
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1274**	N/A	O-MIC-WIND-230919/747
Information Exposure	11-09-2019	2.1	An information disclosure exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle sandbox	N/A	O-MIC-WIND-230919/748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			checks, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1282**		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1256. **CVE ID : CVE-2019-1285**	N/A	O-MIC-WIND-230919/749
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1252. **CVE ID : CVE-2019-1286**	N/A	O-MIC-WIND-230919/750
Improper Input Validation	11-09-2019	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connectivity Assistant handles objects in memory, aka 'Windows Network Connectivity Assistant Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1287**	N/A	O-MIC-WIND-230919/751
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects	N/A	O-MIC-WIND-230919/752

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1291. **CVE ID : CVE-2019-1290**		
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1290. **CVE ID : CVE-2019-1291**	N/A	O-MIC-WIND-230919/753
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists in Windows when the Windows SMB Client kernel-mode driver fails to properly handle objects in memory, aka 'Windows SMB Client Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1293**	N/A	O-MIC-WIND-230919/754
windows_server_2016					
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-230919/755

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2019-1071, CVE-2019-1073. **CVE ID : CVE-2019-1125**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249. **CVE ID : CVE-2019-1250**	N/A	O-MIC-WIND-230919/756
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1244, CVE-2019-1245. **CVE ID : CVE-2019-1251**	N/A	O-MIC-WIND-230919/757
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1286. **CVE ID : CVE-2019-1252**	N/A	O-MIC-WIND-230919/758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1215, CVE-2019-1278, CVE-2019-1303. **CVE ID : CVE-2019-1253**	N/A	O-MIC-WIND-230919/759
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1280**	N/A	O-MIC-WIND-230919/760
Improper Input Validation	11-09-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. **CVE ID : CVE-2019-0928**	N/A	O-MIC-WIND-230919/761
Improper Privilege	11-09-2019	7.2	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1214**		230919/762
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in the way that ws2ifsl.sys (Winsock) handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1253, CVE-2019-1278, CVE-2019-1303. **CVE ID : CVE-2019-1215**	N/A	O-MIC-WIND-230919/763
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1216**	N/A	O-MIC-WIND-230919/764
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows Transaction Manager improperly handles objects in memory, aka 'Windows Transaction Manager Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1219**	N/A	O-MIC-WIND-230919/765
Improper Privilege Management	11-09-2019	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly	N/A	O-MIC-WIND-230919/766

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impersonates certain file operations, aka 'Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1232**		
Improper Input Validation	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server process does not validate the source of input or commands it receives, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1235**	N/A	O-MIC-WIND-230919/767
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1208. **CVE ID : CVE-2019-1236**	N/A	O-MIC-WIND-230919/768
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-	N/A	O-MIC-WIND-230919/769

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1250. **CVE ID : CVE-2019-1240**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1241**	N/A	O-MIC-WIND-230919/770
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1242**	N/A	O-MIC-WIND-230919/771
Improper Restriction of Operations within the Bounds of a Memory	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution	N/A	O-MIC-WIND-230919/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1243**		
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1245, CVE-2019-1251. **CVE ID : CVE-2019-1244**	N/A	O-MIC-WIND-230919/773
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1244, CVE-2019-1251. **CVE ID : CVE-2019-1245**	N/A	O-MIC-WIND-230919/774
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-	N/A	O-MIC-WIND-230919/775

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1246**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1247**	N/A	O-MIC-WIND-230919/776
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1248**	N/A	O-MIC-WIND-230919/777
Improper Restriction of Operations within the	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet	N/A	O-MIC-WIND-230919/778

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer		🟥	Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1250. **CVE ID : CVE-2019-1249**		
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when Windows Hyper-V writes uninitialized memory to disk, aka 'Windows Hyper-V Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1254**	N/A	O-MIC-WIND-230919/779
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1285. **CVE ID : CVE-2019-1256**	N/A	O-MIC-WIND-230919/780
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Compatibility Appraiser where a configuration file, with local privileges, is vulnerable to symbolic link and hard link attacks, aka 'Microsoft Compatibility Appraiser Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-230919/781

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1267		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists when Winlogon does not properly handle file path information, aka 'Winlogon Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1268**	N/A	O-MIC-WIND-230919/782
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1272. **CVE ID : CVE-2019-1269**	N/A	O-MIC-WIND-230919/783
Improper Privilege Management	11-09-2019	3.6	An elevation of privilege vulnerability exists in Windows store installer where WindowsApps directory is vulnerable to symbolic link attack, aka 'Microsoft Windows Store Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1270**	N/A	O-MIC-WIND-230919/784
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists in hdAudio.sys which may lead to an out of band write, aka 'Windows Media Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-230919/785

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1271		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1269. **CVE ID : CVE-2019-1272**	N/A	O-MIC-WIND-230919/786
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when Active Directory Federation Services (ADFS) does not properly sanitize certain error messages, aka 'Active Directory Federation Services XSS Vulnerability'. **CVE ID : CVE-2019-1273**	N/A	O-MIC-WIND-230919/787
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1274**	N/A	O-MIC-WIND-230919/788
Improper Privilege Management	11-09-2019	4.6	An elevation of privilege vulnerability exists in Windows Audio Service when a malformed parameter is processed, aka 'Windows Audio Service Elevation of Privilege	N/A	O-MIC-WIND-230919/789

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2019-1277**		
Improper Privilege Management	11-09-2019	4.6	An elevation of privilege vulnerability exists in the way that the unistore.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1215, CVE-2019-1253, CVE-2019-1303. **CVE ID : CVE-2019-1278**	N/A	O-MIC-WIND-230919/790
Information Exposure	11-09-2019	2.1	An information disclosure exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle sandbox checks, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1282**	N/A	O-MIC-WIND-230919/791
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1256. **CVE ID : CVE-2019-1285**	N/A	O-MIC-WIND-230919/792
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-230919/793

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2019-1252. **CVE ID : CVE-2019-1286**		
Improper Input Validation	11-09-2019	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connectivity Assistant handles objects in memory, aka 'Windows Network Connectivity Assistant Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1287**	N/A	O-MIC-WIND-230919/794
Improper Privilege Management	11-09-2019	3.6	An elevation of privilege vulnerability exists when the Windows Update Delivery Optimization does not properly enforce file share permissions, aka 'Windows Update Delivery Optimization Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1289**	N/A	O-MIC-WIND-230919/795
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1291. **CVE ID : CVE-2019-1290**	N/A	O-MIC-WIND-230919/796
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects	N/A	O-MIC-WIND-230919/797

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1290. **CVE ID : CVE-2019-1291**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	6.8	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-1292**	N/A	O-MIC-WIND-230919/798
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists in Windows when the Windows SMB Client kernel-mode driver fails to properly handle objects in memory, aka 'Windows SMB Client Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1293**	N/A	O-MIC-WIND-230919/799
Improper Input Validation	11-09-2019	2.1	A security feature bypass exists when Windows Secure Boot improperly restricts access to debugging functionality, aka 'Windows Secure Boot Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1294**	N/A	O-MIC-WIND-230919/800
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions.To exploit this	N/A	O-MIC-WIND-230919/801

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1215, CVE-2019-1253, CVE-2019-1278. **CVE ID : CVE-2019-1303**		
windows_server_2019					
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073. **CVE ID : CVE-2019-1125**	N/A	O-MIC-WIND-230919/802
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249. **CVE ID : CVE-2019-1250**	N/A	O-MIC-WIND-230919/803
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when	N/A	O-MIC-WIND-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1244, CVE-2019-1245. **CVE ID : CVE-2019-1251**		230919/804
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1286. **CVE ID : CVE-2019-1252**	N/A	O-MIC-WIND-230919/805
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1215, CVE-2019-1278, CVE-2019-1303. **CVE ID : CVE-2019-1253**	N/A	O-MIC-WIND-230919/806
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who	N/A	O-MIC-WIND-230919/807

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1280**		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1214**	N/A	O-MIC-WIND-230919/808
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in the way that ws2ifsl.sys (Winsock) handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1253, CVE-2019-1278, CVE-2019-1303. **CVE ID : CVE-2019-1215**	N/A	O-MIC-WIND-230919/809
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows Transaction Manager improperly handles objects in memory, aka 'Windows Transaction Manager Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1219**	N/A	O-MIC-WIND-230919/810
Improper Privilege	11-09-2019	4.6	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard	N/A	O-MIC-WIND-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Collector Service improperly impersonates certain file operations, aka 'Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1232**		230919/811
Improper Input Validation	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows Text Service Framework (TSF) when the TSF server process does not validate the source of input or commands it receives, aka 'Windows Text Service Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1235**	N/A	O-MIC-WIND-230919/812
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1208. **CVE ID : CVE-2019-1236**	N/A	O-MIC-WIND-230919/813
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248,	N/A	O-MIC-WIND-230919/814

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1240**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1241**	N/A	O-MIC-WIND-230919/815
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1242**	N/A	O-MIC-WIND-230919/816
Improper Restriction of Operations within the Bounds of a	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote	N/A	O-MIC-WIND-230919/817

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1243**		
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1245, CVE-2019-1251. **CVE ID : CVE-2019-1244**	N/A	O-MIC-WIND-230919/818
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1244, CVE-2019-1251. **CVE ID : CVE-2019-1245**	N/A	O-MIC-WIND-230919/819
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-	N/A	O-MIC-WIND-230919/820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1242, CVE-2019-1243, CVE-2019-1247, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1246**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1248, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1247**	N/A	O-MIC-WIND-230919/821
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1249, CVE-2019-1250. **CVE ID : CVE-2019-1248**	N/A	O-MIC-WIND-230919/822
Improper Restriction of Operations	11-09-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles	N/A	O-MIC-WIND-230919/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1240, CVE-2019-1241, CVE-2019-1242, CVE-2019-1243, CVE-2019-1246, CVE-2019-1247, CVE-2019-1248, CVE-2019-1250. **CVE ID : CVE-2019-1249**		
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when Windows Hyper-V writes uninitialized memory to disk, aka 'Windows Hyper-V Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1254**	N/A	O-MIC-WIND-230919/824
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1285. **CVE ID : CVE-2019-1256**	N/A	O-MIC-WIND-230919/825
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Microsoft Compatibility Appraiser where a configuration file, with local privileges, is vulnerable to symbolic link and hard link attacks, aka 'Microsoft Compatibility Appraiser Elevation of Privilege	N/A	O-MIC-WIND-230919/826

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2019-1267**		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists when Winlogon does not properly handle file path information, aka 'Winlogon Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1268**	N/A	O-MIC-WIND-230919/827
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1272. **CVE ID : CVE-2019-1269**	N/A	O-MIC-WIND-230919/828
Improper Privilege Management	11-09-2019	3.6	An elevation of privilege vulnerability exists in Windows store installer where WindowsApps directory is vulnerable to symbolic link attack, aka 'Microsoft Windows Store Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1270**	N/A	O-MIC-WIND-230919/829
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege exists in hdAudio.sys which may lead to an out of band write, aka 'Windows Media Elevation of Privilege	N/A	O-MIC-WIND-230919/830

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2019-1271**		
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1269. **CVE ID : CVE-2019-1272**	N/A	O-MIC-WIND-230919/831
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-09-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when Active Directory Federation Services (ADFS) does not properly sanitize certain error messages, aka 'Active Directory Federation Services XSS Vulnerability'. **CVE ID : CVE-2019-1273**	N/A	O-MIC-WIND-230919/832
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1274**	N/A	O-MIC-WIND-230919/833
Improper Privilege Management	11-09-2019	4.6	An elevation of privilege vulnerability exists in Windows Audio Service when a malformed parameter is processed, aka 'Windows Audio Service	N/A	O-MIC-WIND-230919/834

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1277**		
Improper Privilege Management	11-09-2019	4.6	An elevation of privilege vulnerability exists in the way that the unistore.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1215, CVE-2019-1253, CVE-2019-1303. **CVE ID : CVE-2019-1278**	N/A	O-MIC-WIND-230919/835
Information Exposure	11-09-2019	2.1	An information disclosure exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle sandbox checks, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1282**	N/A	O-MIC-WIND-230919/836
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1256. **CVE ID : CVE-2019-1285**	N/A	O-MIC-WIND-230919/837
Information Exposure	11-09-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information	N/A	O-MIC-WIND-230919/838

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1252. **CVE ID : CVE-2019-1286**		
Improper Input Validation	11-09-2019	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connectivity Assistant handles objects in memory, aka 'Windows Network Connectivity Assistant Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1287**	N/A	O-MIC-WIND-230919/839
Improper Privilege Management	11-09-2019	3.6	An elevation of privilege vulnerability exists when the Windows Update Delivery Optimization does not properly enforce file share permissions, aka 'Windows Update Delivery Optimization Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1289**	N/A	O-MIC-WIND-230919/840
Improper Input Validation	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1291. **CVE ID : CVE-2019-1290**	N/A	O-MIC-WIND-230919/841
Improper Input	11-09-2019	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop	N/A	O-MIC-WIND-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0787, CVE-2019-0788, CVE-2019-1290. **CVE ID : CVE-2019-1291**		230919/842
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-09-2019	6.8	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-1292**	N/A	O-MIC-WIND-230919/843
Information Exposure	11-09-2019	2.1	An information disclosure vulnerability exists in Windows when the Windows SMB Client kernel-mode driver fails to properly handle objects in memory, aka 'Windows SMB Client Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1293**	N/A	O-MIC-WIND-230919/844
Improper Input Validation	11-09-2019	2.1	A security feature bypass exists when Windows Secure Boot improperly restricts access to debugging functionality, aka 'Windows Secure Boot Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1294**	N/A	O-MIC-WIND-230919/845
Improper Privilege Management	11-09-2019	7.2	An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles	N/A	O-MIC-WIND-230919/846

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1215, CVE-2019-1253, CVE-2019-1278. **CVE ID : CVE-2019-1303**		
Netgear					
wnr2000_firmware					
NULL Pointer Dereference	11-09-2019	5	An exploitable denial-of-service vulnerability exists in the session handling functionality of the NETGEAR N300 (WNR2000v5 with Firmware Version V1.0.0.70) HTTP server. An HTTP request with an empty User-Agent string sent to a page requiring authentication can cause a null pointer dereference, resulting in the HTTP service crashing. An unauthenticated attacker can send a specially crafted HTTP request to trigger this vulnerability. **CVE ID : CVE-2019-5054**	N/A	O-NET-WNR2-230919/847
NULL Pointer Dereference	11-09-2019	5	An exploitable denial-of-service vulnerability exists in the Host Access Point Daemon (hostapd) on the NETGEAR N300 (WNR2000v5 with Firmware Version V1.0.0.70) wireless router. A SOAP request sent	N/A	O-NET-WNR2-230919/848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in an invalid sequence to the <WFAWLANConfig:1#PutMessage> service can cause a null pointer dereference, resulting in the hostapd service crashing. An unauthenticated attacker can send a specially-crafted SOAP request to trigger this vulnerability. **CVE ID : CVE-2019-5055**		
Philips					
hdi_4000_firmware					
Information Exposure	04-09-2019	3.6	In Philips HDI 4000 Ultrasound Systems, all versions running on old, unsupported operating systems such as Windows 2000, the HDI 4000 Ultrasound System is built on an old operating system that is no longer supported. Thus, any unmitigated vulnerability in the old operating system could be exploited to affect this product. **CVE ID : CVE-2019-10988**	N/A	O-PHI-HDI_-230919/849
Redhat					
enterprise_linux_desktop					
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071,	N/A	O-RED-ENTE-230919/850

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-1073. **CVE ID : CVE-2019-1125**		
N/A	06-09-2019	7.5	A flaw was found in ghostscript, versions 9.x before 9.28, in the setsystemparams procedure where it did not properly secure its privileged calls, enabling scripts to bypass `-dSAFER` restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands. **CVE ID : CVE-2019-14813**	N/A	O-RED-ENTE-230919/851
enterprise_linux_server					
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073. **CVE ID : CVE-2019-1125**	N/A	O-RED-ENTE-230919/852
N/A	06-09-2019	7.5	A flaw was found in ghostscript, versions 9.x before 9.28, in the setsystemparams procedure where it did not properly secure its privileged calls, enabling scripts to bypass `-dSAFER` restrictions. A specially crafted PostScript file could disable security protection and then have	N/A	O-RED-ENTE-230919/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the file system, or execute arbitrary commands. **CVE ID : CVE-2019-14813**		
enterprise_linux_server_aus					
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073. **CVE ID : CVE-2019-1125**	N/A	O-RED-ENTE-230919/854
N/A	06-09-2019	7.5	A flaw was found in ghostscript, versions 9.x before 9.28, in the setsystemparams procedure where it did not properly secure its privileged calls, enabling scripts to bypass `-dSAFER` restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands. **CVE ID : CVE-2019-14813**	N/A	O-RED-ENTE-230919/855
enterprise_linux_server_eus					
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071,	N/A	O-RED-ENTE-230919/856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-1073. **CVE ID : CVE-2019-1125**		
N/A	06-09-2019	7.5	A flaw was found in ghostscript, versions 9.x before 9.28, in the setsystemparams procedure where it did not properly secure its privileged calls, enabling scripts to bypass `-dSAFER` restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands. **CVE ID : CVE-2019-14813**	N/A	O-RED-ENTE-230919/857
enterprise_linux_server_tus					
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073. **CVE ID : CVE-2019-1125**	N/A	O-RED-ENTE-230919/858
N/A	06-09-2019	7.5	A flaw was found in ghostscript, versions 9.x before 9.28, in the setsystemparams procedure where it did not properly secure its privileged calls, enabling scripts to bypass `-dSAFER` restrictions. A specially crafted PostScript file could disable security protection and then have	N/A	O-RED-ENTE-230919/859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the file system, or execute arbitrary commands. **CVE ID : CVE-2019-14813**		
enterprise_linux_workstation					
Information Exposure	03-09-2019	2.1	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073. **CVE ID : CVE-2019-1125**	N/A	O-RED-ENTE-230919/860
N/A	06-09-2019	7.5	A flaw was found in ghostscript, versions 9.x before 9.28, in the setsystemparams procedure where it did not properly secure its privileged calls, enabling scripts to bypass `-dSAFER` restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands. **CVE ID : CVE-2019-14813**	N/A	O-RED-ENTE-230919/861
enterprise_linux					
N/A	06-09-2019	7.5	A flaw was found in ghostscript, versions 9.x before 9.28, in the setsystemparams procedure where it did not properly secure its privileged calls, enabling scripts to bypass `-dSAFER` restrictions. A specially crafted PostScript	N/A	O-RED-ENTE-230919/862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file could disable security protection and then have access to the file system, or execute arbitrary commands. **CVE ID : CVE-2019-14813**		
Silver-peak					
unity_edgeconnect_sd-wan_firmware					
Cross-Site Request Forgery (CSRF)	08-09-2019	6.8	Silver Peak EdgeConnect SD-WAN before 8.1.7.x allows CSRF via JSON data to a .swf file. **CVE ID : CVE-2019-16099**	N/A	O-SIL-UNIT-230919/863
Improper Input Validation	08-09-2019	5	Silver Peak EdgeConnect SD-WAN before 8.1.7.x allows remote attackers to trigger a web-interface outage via slow client-side HTTP traffic from a single source. **CVE ID : CVE-2019-16100**	N/A	O-SIL-UNIT-230919/864
Information Exposure	08-09-2019	5	Silver Peak EdgeConnect SD-WAN before 8.1.7.x allows remote attackers to obtain potentially sensitive stack traces by sending incorrect JSON data to the REST API, such as the rest/json/banners URI. **CVE ID : CVE-2019-16101**	N/A	O-SIL-UNIT-230919/865
Improper Input Validation	08-09-2019	7.5	Silver Peak EdgeConnect SD-WAN before 8.1.7.x has an SNMP service with a public value for rocommunity and trapcommunity. **CVE ID : CVE-2019-16102**	N/A	O-SIL-UNIT-230919/866
N/A	08-09-2019	9	Silver Peak EdgeConnect SD-WAN before 8.1.7.x allows privilege escalation (by	N/A	O-SIL-UNIT-230919/867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrators) from the menu to a root Bash OS shell via the spsshell feature. **CVE ID : CVE-2019-16103**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-09-2019	4.3	Silver Peak EdgeConnect SD-WAN before 8.1.7.x has reflected XSS via the rest/json/configdb/download/ PATH_INFO. **CVE ID : CVE-2019-16104**	N/A	O-SIL-UNIT-230919/868
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-09-2019	4	Silver Peak EdgeConnect SD-WAN before 8.1.7.x allows ..%2f directory traversal via a rest/json/configdb/download/ URI. **CVE ID : CVE-2019-16105**	N/A	O-SIL-UNIT-230919/869
smanos					
w100_firmware					
N/A	05-09-2019	3.3	Smanos W100 1.0.0 devices have Insecure Permissions, exploitable by an attacker on the same Wi-Fi network. **CVE ID : CVE-2019-13361**	N/A	O-SMA-W100-230919/870
telestar					
bobs_rock_radio_firmware					
Use of Hard-coded Credentials	11-09-2019	10	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have an	N/A	O-TEL-BOBS-230919/871

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			undocumented TELNET service within the BusyBox subsystem, leading to root access. **CVE ID : CVE-2019-13473**		
dabman_d10_firmware					
Use of Hard-coded Credentials	11-09-2019	10	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have an undocumented TELNET service within the BusyBox subsystem, leading to root access. **CVE ID : CVE-2019-13473**	N/A	O-TEL-DABM-230919/872
dabman_i30_stereo_firmware					
Use of Hard-coded Credentials	11-09-2019	10	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have an undocumented TELNET service within the BusyBox subsystem, leading to root access. **CVE ID : CVE-2019-13473**	N/A	O-TEL-DABM-230919/873
imperial_i110_firmware					
Use of Hard-coded	11-09-2019	10	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30	N/A	O-TEL-IMPE-230919/874

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have an undocumented TELNET service within the BusyBox subsystem, leading to root access. **CVE ID : CVE-2019-13473**		
imperial_i150_firmware					
Use of Hard-coded Credentials	11-09-2019	10	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have an undocumented TELNET service within the BusyBox subsystem, leading to root access. **CVE ID : CVE-2019-13473**	N/A	O-TEL-IMPE-230919/875
imperial_i200-cd_firmware					
Use of Hard-coded Credentials	11-09-2019	10	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have an undocumented TELNET service within the BusyBox	N/A	O-TEL-IMPE-230919/876

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subsystem, leading to root access. **CVE ID : CVE-2019-13473**		
imperial_i200_firmware					
Use of Hard-coded Credentials	11-09-2019	10	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have an undocumented TELNET service within the BusyBox subsystem, leading to root access. **CVE ID : CVE-2019-13473**	N/A	O-TEL-IMPE-230919/877
imperial_i400_firmware					
Use of Hard-coded Credentials	11-09-2019	10	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have an undocumented TELNET service within the BusyBox subsystem, leading to root access. **CVE ID : CVE-2019-13473**	N/A	O-TEL-IMPE-230919/878
imperial_i450_firmware					
Use of Hard-coded Credentials	11-09-2019	10	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200,	N/A	O-TEL-IMPE-230919/879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have an undocumented TELNET service within the BusyBox subsystem, leading to root access. **CVE ID : CVE-2019-13473**		
imperial_i500-bt_firmware					
Use of Hard-coded Credentials	11-09-2019	10	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have an undocumented TELNET service within the BusyBox subsystem, leading to root access. **CVE ID : CVE-2019-13473**	N/A	O-TEL-IMPE-230919/880
imperial_i600_firmware					
Use of Hard-coded Credentials	11-09-2019	10	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have an undocumented TELNET service within the BusyBox subsystem, leading to root access.	N/A	O-TEL-IMPE-230919/881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-13473		
tripplite					
pdumh15at_firmware					
Improper Authentication	12-09-2019	8.5	Tripp Lite PDUMH15AT 12.04.0053 devices allow unauthenticated POST requests to the /Forms/ directory, as demonstrated by changing the manager or admin password, or shutting off power to an outlet. NOTE: the vendor's position is that a newer firmware version, fixing this vulnerability, had already been released before this vulnerability report about 12.04.0053. **CVE ID : CVE-2019-16261**	N/A	O-TRI-PDUM-230919/882
xiaoyi					
yi_m1_mirrorless_camera_firmware					
Improper Authentication	06-09-2019	8.3	An exploitable authentication bypass vulnerability exists in the Bluetooth Low Energy (BLE) authentication module of YI M1 Mirrorless Camera V3.2-cn. An attacker can send a set of BLE commands to trigger this vulnerability, resulting in sensitive data leakage (e.g., personal photos). An attacker can also control the camera to record or take a picture after bypassing authentication. **CVE ID : CVE-2019-13953**	N/A	O-XIA-YI_M-230919/883
Xilinx					
zynq_ultrascale+_mpsoc_firmware					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	03-09-2019	2.1	A weakness was found in Encrypt Only boot mode in Zynq UltraScale+ devices. This could lead to an adversary being able to modify the control fields of the boot image leading to an incorrect secure boot behavior. **CVE ID : CVE-2019-5478**	N/A	O-XIL-ZYNQ-230919/884
zynq_ultrascale+_rfsoc_firmware					
Improper Input Validation	03-09-2019	2.1	A weakness was found in Encrypt Only boot mode in Zynq UltraScale+ devices. This could lead to an adversary being able to modify the control fields of the boot image leading to an incorrect secure boot behavior. **CVE ID : CVE-2019-5478**	N/A	O-XIL-ZYNQ-230919/885