National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Jun 2019 Vol. 06 No. 11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Adobe					
flash_player					
Use After Free	12-06-2019	6.8	Adobe Flash Player versions 32.0.0.192 and earlier, 32.0.0.192 and earlier, and 32.0.0.192 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7845**	https://helpx.adobe.com/security/products/flash-player/apsb19-30.html	A-ADO-FLAS-210619/1
coldfusion					
Unrestricted Upload of File with Dangerous Type	12-06-2019	10	ColdFusion versions Update 3 and earlier, Update 10 and earlier, and Update 18 and earlier have a file extension blacklist bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7838**	https://helpx.adobe.com/security/products/coldfusion/apsb19-27.html	A-ADO-COLD-210619/2
Improper Neutralization of Special Elements used in a Command ('Command Injection')	12-06-2019	10	ColdFusion versions Update 3 and earlier, Update 10 and earlier, and Update 18 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7839**	https://helpx.adobe.com/security/products/coldfusion/apsb19-27.html	A-ADO-COLD-210619/3
Deserialization of	12-06-2019	10	ColdFusion versions Update 3 and earlier, Update 10 and	https://helpx.adobe.c	A-ADO-COLD-

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
Untrusted Data			earlier, and Update 18 and earlier have a deserialization of untrusted data vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2019-7840**	om/security/products/coldfusion/apsb19-27.html	210619/4
Apache					
http_server					
Use After Free	11-06-2019	5	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly. **CVE ID : CVE-2019-0196**	N/A	A-APA-HTTP-210619/5
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	11-06-2019	4.9	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue. **CVE ID : CVE-2019-0197**	https://support.f5.com/csp/article/K44591505	A-APA-HTTP-210619/6
N/A	11-06-2019	5	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'),	N/A	A-APA-HTTP-210619/7

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
			directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them. **CVE ID : CVE-2019-0220**		
apcupsd					
apcupsd					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-06-2019	4.3	Apcupsd 0.3.91_5, as used in pfSense through 2.4.4-RELEASE-p3 and other products, has an XSS issue in apcupsd_status.php. **CVE ID : CVE-2019-12584**	N/A	A-APC-APCU-210619/8
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-06-2019	7.5	Apcupsd 0.3.91_5, as used in pfSense through 2.4.4-RELEASE-p3 and other products, has an Arbitrary Command Execution issue in apcupsd_status.php. **CVE ID : CVE-2019-12585**	N/A	A-APC-APCU-210619/9
api_based_travel_booking_project					
api_based_travel_booking					
Improper Neutralization of Input During	06-06-2019	4.3	An issue was discovered in PHP Scripts Mall API Based Travel Booking 3.4.7. There is Reflected XSS via the flight-results.php d2	N/A	A-API-API_-210619/10

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
Web Page Generation ('Cross-site Scripting')			parameter. **CVE ID : CVE-2019-7554**		
Artifex					
mupdf					
NULL Pointer Dereference	13-06-2019	7.5	Usage of an uninitialized variable in the function fz_load_jpeg in Artifex MuPDF 1.14 can result in a heap overflow vulnerability that allows an attacker to execute arbitrary code. **CVE ID : CVE-2019-7321**	N/A	A-ART-MUPD-210619/11
mujs					
Incorrect Regular Expression	13-06-2019	7.5	An issue was discovered in Artifex MuJS 1.0.5. regcompx in regexp.c does not restrict regular expression program size, leading to an overflow of the parsed syntax list size. **CVE ID : CVE-2019-12798**	N/A	A-ART-MUJS-210619/12
Atlassian					
bitbucket					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-06-2019	9	Atlassian Bitbucket Data Center licensed instances starting with version 5.13.0 before 5.13.6 (the fixed version for 5.13.x), from 5.14.0 before 5.14.4 (fixed version for 5.14.x), from 5.15.0 before 5.15.3 (fixed version for 5.15.x), from 5.16.0 before 5.16.3 (fixed version for 5.16.x), from 6.0.0 before 6.0.3 (fixed version for 6.0.x), and from 6.1.0 before 6.1.2 (the fixed version for 6.1.x) allow remote attackers who have	N/A	A-ATL-BITB-210619/13

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
			admin permissions to achieve remote code execution on a Bitbucket server instance via path traversal through the Data Center migration tool. **CVE ID : CVE-2019-3397**		
crowd					
Improper Input Validation	03-06-2019	7.5	Atlassian Crowd and Crowd Data Center had the pdkinstall development plugin incorrectly enabled in release builds. Attackers who can send unauthenticated or authenticated requests to a Crowd or Crowd Data Center instance can exploit this vulnerability to install arbitrary plugins, which permits remote code execution on systems running a vulnerable version of Crowd or Crowd Data Center. All versions of Crowd from version 2.1.0 before 3.0.5 (the fixed version for 3.0.x), from version 3.1.0 before 3.1.6 (the fixed version for 3.1.x), from version 3.2.0 before 3.2.8 (the fixed version for 3.2.x), from version 3.3.0 before 3.3.5 (the fixed version for 3.3.x), and from version 3.4.0 before 3.4.4 (the fixed version for 3.4.x) are affected by this vulnerability. **CVE ID : CVE-2019-11580**	N/A	A-ATL-CROW-210619/14
Atutor					
atutor					
Unrestricted Upload of File with	03-06-2019	6.8	ATutor 2.2.4 allows Arbitrary File Upload and Directory Traversal, resulting in remote code execution via a ".." pathname in a	N/A	A-ATU-ATUT-210619/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			ZIP archive to the mods/_core/languages/language_import.php (aka Import New Language) or mods/_standard/patcher/index_admin.php (aka Patcher) component. **CVE ID : CVE-2019-12169**		
bevywise					
mqttroute					
Improper Input Validation	10-06-2019	5	In Bevywise MQTTRoute 1.1 build 1018-002, a connect packet combined with a malformed unsubscribe request packet can be used to cause a Denial of Service attack against the broker. **CVE ID : CVE-2019-6241**	N/A	A-BEV-MQTT-210619/16
Bitdefender					
safepay					
Improper Input Validation	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Bitdefender SafePay 23.0.10.34. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of tiscript. When processing the System.Exec method the application does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-	N/A	A-BIT-SAFE-210619/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7234. **CVE ID : CVE-2019-6736**		
N/A	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Bitdefender SafePay 23.0.10.34. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of TIScript. The issue lies in the handling of the openFile method, which allows for an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability execute code in the context of the current process. Was ZDI-CAN-7247. **CVE ID : CVE-2019-6737**	N/A	A-BIT-SAFE-210619/18
Improper Input Validation	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Bitdefender SafePay 23.0.10.34. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of TIScript. When processing the launch method the application does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability execute code in the context of the current process. Was ZDI-CAN-7250.	N/A	A-BIT-SAFE-210619/19

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-2019-6738		
bludit					
bludit					
Improper Control of Generation of Code ('Code Injection')	03-06-2019	6.5	Bludit before 3.9.0 allows remote code execution for an authenticated user by uploading a php file while changing the logo through /admin/ajax/upload-logo. **CVE ID : CVE-2019-12548**	https://github.com/bludit/bludit/releases/tag/3.9.0	A-BLU-BLUD-210619/20
Improper Authentication	05-06-2019	6.5	Bludit prior to 3.9.1 allows a non-privileged user to change the password of any account, including admin. This occurs because of bl-kernel/admin/controllers/user-password.php Insecure Direct Object Reference (a modified username POST parameter). **CVE ID : CVE-2019-12742**	N/A	A-BLU-BLUD-210619/21
chartered_accountant_auditor_website_project					
chartered_accountant_auditor_website					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-06-2019	3.5	PHP Scripts Mall Chartered Accountant : Auditor Website 2.0.1 has Stored XSS in the Profile Update page via the My Name field. **CVE ID : CVE-2019-7553**	N/A	A-CHA-CHAR-210619/22
chartkick_gem_project					
chartkick_gem					
Improper Neutraliz	06-06-2019	2.6	The Chartkick gem through 3.1.0 for Ruby allows XSS.	https://github.com/a	A-CHA-CHAR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ation of Input During Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2019-12732**	nkane/chartkick/issues/488	210619/23
Cisco					
webex_meetings_server					
Information Exposure	05-06-2019	5	A vulnerability in the web-based management interface of Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to access sensitive system information. The vulnerability is due to improper access control to files within the web-based management interface. An attacker could exploit this vulnerability by sending a malicious request to an affected device. A successful exploit could allow the attacker to access sensitive system information. **CVE ID : CVE-2019-1868**	N/A	A-CIS-WEBE-210619/24
unified_communications_manager_im_and_presence_service					
Improper Input Validation	05-06-2019	5	A vulnerability in the authentication service of the Cisco Unified Communications Manager IM and Presence (Unified CM IM&P) Service, Cisco TelePresence Video Communication Server (VCS), and Cisco Expressway Series could allow an unauthenticated, remote attacker to cause a	N/A	A-CIS-UNIF-210619/25

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service outage for users attempting to authenticate, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient controls for specific memory operations. An attacker could exploit this vulnerability by sending a malformed Extensible Messaging and Presence Protocol (XMPP) authentication request to an affected system. A successful exploit could allow the attacker to cause an unexpected restart of the authentication service, preventing users from successfully authenticating. Exploitation of this vulnerability does not impact users who were authenticated prior to an attack. **CVE ID : CVE-2019-1845**		
industrial_network_director					
Cross-Site Request Forgery (CSRF)	05-06-2019	6.8	A vulnerability in the web-based management interface of Cisco Industrial Network Director (IND) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to use a web browser	N/A	A-CIS-INDU-210619/26

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 the privileges of the user to perform arbitrary actions on an affected device. For more information about CSRF attacks and potential mitigations, see Understanding Cross-Site Request Forgery Threat Vectors. **CVE ID : CVE-2019-1881**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-06-2019	3.5	A vulnerability in Cisco Industrial Network Director could allow an authenticated, remote attacker to conduct stored cross-site scripting (XSS) attacks. The vulnerability is due to improper validation of content submitted to the affected application. An attacker could exploit this vulnerability by sending requests containing malicious values to the affected system. A successful exploit could allow the attacker to conduct XSS attacks. **CVE ID : CVE-2019-1882**	N/A	A-CIS-INDU-210619/27
telepresence_video_communication_server					
Server-Side Request Forgery (SSRF)	05-06-2019	5	A vulnerability in Cisco TelePresence Video Communication Server (VCS) and Cisco Expressway Series software could allow an unauthenticated, remote attacker to cause an affected system to send arbitrary network requests. The vulnerability is due to improper restrictions on network services in the affected software. An attacker could exploit this vulnerability by sending malicious requests to the affected system. A successful exploit could allow the attacker to send	N/A	A-CIS-TELE-210619/28

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
			arbitrary network requests sourced from the affected system. **CVE ID : CVE-2019-1872**		
Improper Input Validation	05-06-2019	5	A vulnerability in the authentication service of the Cisco Unified Communications Manager IM and Presence (Unified CM IM&P) Service, Cisco TelePresence Video Communication Server (VCS), and Cisco Expressway Series could allow an unauthenticated, remote attacker to cause a service outage for users attempting to authenticate, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient controls for specific memory operations. An attacker could exploit this vulnerability by sending a malformed Extensible Messaging and Presence Protocol (XMPP) authentication request to an affected system. A successful exploit could allow the attacker to cause an unexpected restart of the authentication service, preventing users from successfully authenticating. Exploitation of this vulnerability does not impact users who were authenticated prior to an attack. **CVE ID : CVE-2019-1845**	N/A	A-CIS-TELE-210619/29
enterprise_chat_and_email					
Improper Neutralization of Input During	05-06-2019	4.3	A vulnerability in the web-based management interface of Cisco Enterprise Chat and Email (ECE) Center could allow an unauthenticated, remote attacker	N/A	A-CIS-ENTE-210619/30

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
Web Page Generation ('Cross-site Scripting')			to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web interface or allow the attacker to access sensitive browser-based information. **CVE ID : CVE-2019-1870**		
Clusterlabs					
libqb					
Improper Link Resolution Before File Access ('Link Following')	07-06-2019	6.6	libqb before 1.0.5 allows local users to overwrite arbitrary files via a symlink attack, because it uses predictable filenames (under /dev/shm and /tmp) without O_EXCL. **CVE ID : CVE-2019-12779**	N/A	A-CLU-LIBQ-210619/31
Cmsmadesimple					
cms_made_simple					
Improper Neutralization of Input During Web Page Generatio	05-06-2019	3.5	CMS Made Simple 2.2.10 has XSS via the m1_name parameter in "Add Article" under Content -> Content Manager -> News. **CVE ID : CVE-2019-11226**	N/A	A-CMS-CMS_-210619/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n ('Cross-site Scripting')					
Cyrus					
imap					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2019	7.5	The CalDAV feature in httpd in Cyrus IMAP 2.5.x through 2.5.12 and 3.0.x through 3.0.9 allows remote attackers to execute arbitrary code via a crafted HTTP PUT operation for an event with a long iCalendar property name. **CVE ID : CVE-2019-11356**	N/A	A-CYR-IMAP-210619/33
Dameware					
remote_mini_control					
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-06-2019	5	Dameware Remote Mini Control version 12.1.0.34 and prior contains a unauthenticated remote heap overflow due to the server not properly validating RsaPubKeyLen during key negotiation. An unauthenticated remote attacker can cause a heap buffer overflow by specifying a large RsaPubKeyLen, which could cause a denial of service. **CVE ID : CVE-2019-3955**	N/A	A-DAM-REMO-210619/34
Out-of-bounds Read	07-06-2019	5.8	Dameware Remote Mini Control version 12.1.0.34 and prior contains an unauthenticated remote buffer over-read due to the server not properly validating CltDHPubKeyLen during key negotiation, which could crash the application or leak sensitive	N/A	A-DAM-REMO-210619/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information. **CVE ID : CVE-2019-3956**		
Out-of-bounds Read	07-06-2019	5.8	Dameware Remote Mini Control version 12.1.0.34 and prior contains an unauthenticated remote buffer over-read due to the server not properly validating RsaSignatureLen during key negotiation, which could crash the application or leak sensitive information. **CVE ID : CVE-2019-3957**	N/A	A-DAM-REMO-210619/36
Dell					
emc_openmanage_server_administrator					
Improper Restriction of XML External Entity Reference ('XXE')	06-06-2019	5	Dell EMC OpenManage Server Administrator (OMSA) versions prior to 9.1.0.3 and prior to 9.2.0.4 contain an XML external entity (XXE) injection vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to read arbitrary server system files by supplying specially crafted document type definitions (DTDs) in an XML request. **CVE ID : CVE-2019-3722**	https://www.dell.com/support/article/us/en/04/sln317441/dsa-2019-074-dell-emc-openmanage-server-administrator-multiple-vulnerabilities?lang=en	A-DEL-EMC_-210619/37
Improper Input Validation	06-06-2019	6.4	Dell EMC OpenManage Server Administrator (OMSA) versions prior to 9.1.0.3 and prior to 9.2.0.4 contain a web parameter tampering vulnerability. A remote unauthenticated attacker could potentially manipulate parameters of web requests to	https://www.dell.com/support/article/us/en/04/sln317441/dsa-2019-074-dell-	A-DEL-EMC_-210619/38

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OMSA to create arbitrary files with empty content or delete the contents of any existing file, due to improper input parameter validation **CVE ID : CVE-2019-3723**	emc-openmanage-server-administrator-multiple-vulnerabilities?lang=en	
Djangoproject					
django					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2019	4.3	An issue was discovered in Django 1.11 before 1.11.21, 2.1 before 2.1.9, and 2.2 before 2.2.2. The clickable Current URL value displayed by the AdminURLFieldWidget displays the provided value without validating it as a safe URL. Thus, an unvalidated value stored in the database, or a value provided as a URL query parameter payload, could result in an clickable JavaScript link. **CVE ID : CVE-2019-12308**	https://www.djangoproject.com/weblog/2019/jun/03/security-releases/	A-DJA-DJAN-210619/39
douco					
douphp					
Improper Access Control	02-06-2019	5	In DouCo DouPHP v1.5 Release 20190516, remote attackers can view the database backup file via a brute-force guessing approach for data/backup/DyyyymmddThhmmss.sql filenames. **CVE ID : CVE-2019-12564**	N/A	A-DOU-DOUP-210619/40
Exim					
exim					

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	05-06-2019	7.5	A flaw was found in Exim versions 4.87 to 4.91 (inclusive). Improper validation of recipient address in deliver_message() function in /src/deliver.c may lead to remote command execution. **CVE ID : CVE-2019-10149**	https://www.exim.org/static/doc/security/CVE-2019-10149.txt	A-EXI-EXIM-210619/41
Facebook					
osquery					
Improper Link Resolution Before File Access ('Link Following')	03-06-2019	9.3	In some configurations an attacker can inject a new executable path into the extensions.load file for osquery and hard link a parent folder of a malicious binary to a folder with known 'safe' permissions. Under those circumstances osquery will load said malicious executable with SYSTEM permissions. The solution is to migrate installations to the 'Program Files' directory on Windows which restricts unprivileged write access. This issue affects osquery prior to v3.4.0. **CVE ID : CVE-2019-3567**	N/A	A-FAC-OSQU-210619/42
Fatfreecrm					
fat_free_crm					
Improper Neutralization of Special Elements in Output Used by a Downstream Compone	10-06-2019	4.3	HTML Injection has been discovered in the v0.19.0 version of the Fat Free CRM product via an authenticated request to the /comments URI. **CVE ID : CVE-2019-10226**	N/A	A-FAT-FAT_-210619/43

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
nt ('Injection')					
Ffmpeg					
ffmpeg					
Improper Initialization	04-06-2019	7.5	aa_read_header in libavformat/aadec.c in FFmpeg before 3.2.14 does not check for sscanf failure and consequently allows use of uninitialized variables. **CVE ID : CVE-2019-12730**	N/A	A-FFM-FFMP-210619/44
firejail_project					
firejail					
Improper Access Control	02-06-2019	4.6	In Firejail before 0.9.60, seccomp filters are writable inside the jail, leading to a lack of intended seccomp restrictions for a process that is joined to the jail after a filter has been modified by an attacker. **CVE ID : CVE-2019-12589**	N/A	A-FIR-FIRE-210619/45
Foxitsoftware					
foxit_studio_photo					
Out-of-bounds Read	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Studio Photo 3.6.6. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an	N/A	A-FOX-FOXI-210619/46

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
			allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7634. **CVE ID : CVE-2019-6746**		
Out-of-bounds Write	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Studio Photo 3.6.6. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EZI files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7636. **CVE ID : CVE-2019-6747**	N/A	A-FOX-FOXI-210619/47
Out-of-bounds Write	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Studio Photo 3.6.6. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EZI files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure.	N/A	A-FOX-FOXI-210619/48

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
			An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7637. **CVE ID : CVE-2019-6748**		
Out-of-bounds Write	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Studio Photo 3.6.6. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EZIX files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7638. **CVE ID : CVE-2019-6749**	N/A	A-FOX-FOXI-210619/49
Out-of-bounds Write	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Studio Photo 3.6.6. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EZI files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in	N/A	A-FOX-FOXI-210619/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the context of the current process. Was ZDI-CAN-7639. **CVE ID : CVE-2019-6750**		
Out-of-bounds Write	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Studio Photo 3.6.6.779. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of JPG files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7632. **CVE ID : CVE-2019-6751**	N/A	A-FOX-FOXI-210619/51
foxit_reader					
Information Exposure	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit PhantomPDF 9.3.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF documents. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with	N/A	A-FOX-FOXI-210619/52

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
			other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7620. **CVE ID : CVE-2019-6752**		
Integer Overflow or Wraparound	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.3.0.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Stuff method. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before writing to memory. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7561. **CVE ID : CVE-2019-6753**	N/A	A-FOX-FOXI-210619/53
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.3.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the localFileStorage method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to	N/A	A-FOX-FOXI-210619/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute code in the context of the current process. Was ZDI-CAN-7407. **CVE ID : CVE-2019-6754**		
Out-of-bounds Write	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.3.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7613. **CVE ID : CVE-2019-6755**	N/A	A-FOX-FOXI-210619/55
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit PhantomPDF 9.4.0.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of HTML files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in	N/A	A-FOX-FOXI-210619/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the context of the current process. Was ZDI-CAN-7769. **CVE ID : CVE-2019-6756**		
Use After Free	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7696. **CVE ID : CVE-2019-6757**	N/A	A-FOX-FOXI-210619/57
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.4.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7701.	N/A	A-FOX-FOXI-210619/58

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-2019-6758		
Out-of-bounds Write	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.3.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7614. **CVE ID : CVE-2019-6759**	N/A	A-FOX-FOXI-210619/59
Out-of-bounds Write	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7694. **CVE ID : CVE-2019-6760**	N/A	A-FOX-FOXI-210619/60

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
Use After Free	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.0.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the XFA CXFA_FFDocView object. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7777. **CVE ID : CVE-2019-6761**	N/A	A-FOX-FOXI-210619/61
Use After Free	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit PhantomPDF 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of HTML files to PDF. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7844. **CVE ID : CVE-2019-6762**	N/A	A-FOX-FOXI-210619/62
Use After Free	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary	N/A	A-FOX-FOXI-210619/63

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
			code on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the ToggleFormsDesign method of the Foxit.FoxitReader.Ctl ActiveX object. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7874. **CVE ID : CVE-2019-6763**		
Out-of-bounds Write	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA Template objects. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7972. **CVE ID : CVE-2019-6764**	N/A	A-FOX-FOXI-210619/64
Out-of-bounds	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary	N/A	A-FOX-FOXI-210619/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			code on vulnerable installations of Foxit PhantomPDF 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of HTML files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8170. **CVE ID : CVE-2019-6765**		
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8162. **CVE ID : CVE-2019-6766**	N/A	A-FOX-FOXI-210619/66
Use After	03-06-2019	6.8	This vulnerability allows remote	N/A	A-FOX-FOXI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8163. **CVE ID : CVE-2019-6767**		210619/67
Use After Free	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8164. **CVE ID : CVE-2019-6768**	N/A	A-FOX-FOXI-210619/68
Use After Free	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations	N/A	A-FOX-FOXI-210619/69

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 Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8165. **CVE ID : CVE-2019-6769**		
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the resetForm method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8229. **CVE ID : CVE-2019-6770**	N/A	A-FOX-FOXI-210619/70
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable	N/A	A-FOX-FOXI-210619/71

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
			installations of Foxit Reader 2019.010.20098. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the value property of a Field object within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8230. **CVE ID : CVE-2019-6771**		
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 2019.010.20098. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8231. **CVE ID : CVE-2019-6772**	N/A	A-FOX-FOXI-210619/72

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
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the richValue property of a Field object within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8272. **CVE ID : CVE-2019-6773**	N/A	A-FOX-FOXI-210619/73
phantompdf					
Information Exposure	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit PhantomPDF 9.3.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF documents. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with	N/A	A-FOX-PHAN-210619/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7620. **CVE ID : CVE-2019-6752**		
Integer Overflow or Wraparound	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.3.0.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Stuff method. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before writing to memory. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7561. **CVE ID : CVE-2019-6753**	N/A	A-FOX-PHAN-210619/75
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.3.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the localFileStorage method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to	N/A	A-FOX-PHAN-210619/76

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
			execute code in the context of the current process. Was ZDI-CAN-7407. **CVE ID : CVE-2019-6754**		
Out-of-bounds Write	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.3.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7613. **CVE ID : CVE-2019-6755**	N/A	A-FOX-PHAN-210619/77
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit PhantomPDF 9.4.0.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of HTML files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in	N/A	A-FOX-PHAN-210619/78

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the context of the current process. Was ZDI-CAN-7769. **CVE ID : CVE-2019-6756**		
Use After Free	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7696. **CVE ID : CVE-2019-6757**	N/A	A-FOX-PHAN-210619/79
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.4.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7701.	N/A	A-FOX-PHAN-210619/80

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-2019-6758		
Out-of-bounds Write	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.3.10826. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7614. **CVE ID : CVE-2019-6759**	N/A	A-FOX-PHAN-210619/81
Out-of-bounds Write	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within ConvertToPDF_x86.dll. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7694. **CVE ID : CVE-2019-6760**	N/A	A-FOX-PHAN-210619/82

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
Use After Free	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.0.16811. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the XFA CXFA_FFDocView object. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7777. **CVE ID : CVE-2019-6761**	N/A	A-FOX-PHAN-210619/83
Use After Free	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit PhantomPDF 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of HTML files to PDF. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7844. **CVE ID : CVE-2019-6762**	N/A	A-FOX-PHAN-210619/84
Use After Free	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary	N/A	A-FOX-PHAN-

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 on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the ToggleFormsDesign method of the Foxit.FoxitReader.Ctl ActiveX object. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7874. **CVE ID : CVE-2019-6763**		210619/85
Out-of-bounds Write	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA Template objects. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-7972. **CVE ID : CVE-2019-6764**	N/A	A-FOX-PHAN-210619/86
Out-of-bounds	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary	N/A	A-FOX-PHAN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			code on vulnerable installations of Foxit PhantomPDF 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of HTML files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8170. **CVE ID : CVE-2019-6765**		210619/87
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8162. **CVE ID : CVE-2019-6766**	N/A	A-FOX-PHAN-210619/88
Use After	03-06-2019	6.8	This vulnerability allows remote	N/A	A-FOX-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8163. **CVE ID : CVE-2019-6767**		PHAN-210619/89
Use After Free	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8164. **CVE ID : CVE-2019-6768**	N/A	A-FOX-PHAN-210619/90
Use After Free	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations	N/A	A-FOX-PHAN-210619/91

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 Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8165. **CVE ID : CVE-2019-6769**		
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the resetForm method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8229. **CVE ID : CVE-2019-6770**	N/A	A-FOX-PHAN-210619/92
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable	N/A	A-FOX-PHAN-210619/93

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
			installations of Foxit Reader 2019.010.20098. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the value property of a Field object within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8230. **CVE ID : CVE-2019-6771**		
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 2019.010.20098. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8231. **CVE ID : CVE-2019-6772**	N/A	A-FOX-PHAN-210619/94

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
Use After Free	03-06-2019	4.3	This vulnerability allows remote attackers to disclose sensitive information on vulnerable installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the richValue property of a Field object within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8272. **CVE ID : CVE-2019-6773**	N/A	A-FOX-PHAN-210619/95
freenetproject					
freenet					
N/A	05-06-2019	6.8	Freenet 1483 has a MIME type bypass that allows arbitrary JavaScript execution via a crafted Freenet URI. **CVE ID : CVE-2019-9673**	N/A	A-FRE-FREE-210619/96
fujielectric					
v-server					
Integer Overflow or Wraparound	12-06-2019	5	Fuji Electric V-Server before 6.0.33.0 is vulnerable to denial of service via a crafted UDP message sent to port 8005. An unauthenticated, remote attacker can crash vserver.exe due to an integer overflow in the UDP	N/A	A-FUJ-V-SE-210619/97

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
			message handling logic. **CVE ID : CVE-2019-3946**		
N/A	12-06-2019	5	Fuji Electric V-Server before 6.0.33.0 stores database credentials in project files as plaintext. An attacker that can gain access to the project file can recover the database credentials and gain access to the database server. **CVE ID : CVE-2019-3947**	N/A	A-FUJ-V-SE-210619/98
gardener					
gardener					
Improper Access Control	05-06-2019	5	In Gardener before 0.20.0, incorrect access control in seed clusters allows information disclosure by sending HTTP GET requests from one's own shoot clusters to foreign shoot clusters. This occurs because traffic from shoot to seed via the VPN endpoint is not blocked. **CVE ID : CVE-2019-12494**	https://groups.google.com/forum/#!topic/gardener/pH6dNIEhv-A	A-GAR-GARD-210619/99
gilacms					
gila_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-06-2019	4.3	Gila CMS 1.9.1 has XSS. **CVE ID : CVE-2019-9647**	N/A	A-GIL-GILA-210619/100
glpi_dashboard_project					

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
glpi_dashboard					
Improper Access Control	02-06-2019	7.5	Incorrect access control was discovered in the stdonato Dashboard plugin through 0.9.7 for GLPI, affecting df.php, issue.php, load.php, mem.php, traf.php, and uptime.php in front/sh. **CVE ID : CVE-2019-12530**	N/A	A-GLP-GLPI-210619/101
glyphandcog					
xpdfreader					
Out-of-bounds Read	01-06-2019	5.8	There is an out-of-bounds read vulnerability in the function FlateStream::getChar() located at Stream.cc in Xpdf 4.01.01. It can, for example, be triggered by sending a crafted PDF document to the pdftoppm tool. It might allow an attacker to cause Information Disclosure or a denial of service. **CVE ID : CVE-2019-12515**	N/A	A-GLY-XPDF-210619/102
Gnome					
gvfs					
Improper Authorization	11-06-2019	4.6	daemon/gvfsdaemon.c in gvfsd from GNOME gvfs before 1.38.3, 1.40.x before 1.40.2, and 1.41.x before 1.41.3 opened a private D-Bus server socket without configuring an authorization rule. A local attacker could connect to this server socket and issue D-Bus method calls. (Note that the server socket only accepts a single connection, so the attacker would have to discover the server and connect to the socket before its owner does.)	N/A	A-GNO-GVFS-210619/103

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
			CVE ID : CVE-2019-12795		
Grails					
grails					
Incorrect Resource Transfer Between Spheres	04-06-2019	6.8	Grails before 3.3.10 used cleartext HTTP to resolve the SDKMan notification service. NOTE: users' apps were not resolving dependencies over cleartext HTTP. **CVE ID : CVE-2019-12728**	N/A	A-GRA-GRAI-210619/104
grandnode					
grandnode					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-06-2019	5	A Path Traversal vulnerability in Controllers/LetsEncryptController.cs in LetsEncryptController in GrandNode 4.40 allows remote, unauthenticated attackers to retrieve arbitrary files on the web server via specially crafted LetsEncrypt/Index?fileName= HTTP requests. A patch for this issue was made on 2019-05-30 in GrandNode 4.40. **CVE ID : CVE-2019-12276**	N/A	A-GRA-GRAN-210619/105
hashicorp					
consul					
Improper Access Control	06-06-2019	6.4	HashiCorp Consul 1.4.0 through 1.5.0 has Incorrect Access Control. Keys not matching a specific ACL rule used for prefix matching in a policy can be deleted by a token using that policy even with default deny settings configured. **CVE ID : CVE-2019-12291**	https://github.com/hashicorp/consul/issues/5888	A-HAS-CONS-210619/106
hoteldruid					

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
hoteldruid					
Divide By Zero	07-06-2019	4	In Hoteldruid before 2.3.1, a division by zero was discovered in $num_tabelle in tab_tariffe.php (aka the numtariffa1 parameter) due to the mishandling of non-numeric values, as demonstrated by the /tab_tariffe.php?anno=[YEAR]&numtariffa1=1a URI. It could allow an administrator to conduct remote denial of service (disrupting certain business functions of the product). **CVE ID : CVE-2019-9084**	N/A	A-HOT-HOTE-210619/107
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-06-2019	7.5	HotelDruid before v2.3.1 has SQL Injection via the /visualizza_tabelle.php anno parameter. **CVE ID : CVE-2019-9086**	N/A	A-HOT-HOTE-210619/108
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-06-2019	7.5	HotelDruid before v2.3.1 has SQL Injection via the /tab_tariffe.php numtariffa1 parameter. **CVE ID : CVE-2019-9087**	N/A	A-HOT-HOTE-210619/109
HP					
intelligent_management_center					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5338**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/110
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5339**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/111
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5340**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/112
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5341**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/113

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 in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5342**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/114
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5343**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/115
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5344**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/116
Improper Neutralization of Special	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than	https://support.hpe.com/hpsc/doc/public/	A-HP-INTE-210619/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			version 7.3 E0506P09. **CVE ID : CVE-2019-5345**	display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	
Improper Authentication	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11941**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/118
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11942**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/119
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11943**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/120
Improper Input	05-06-2019	10	A remote code execution vulnerability was identified in	https://support.hpe.c	A-HP-INTE-210619/121

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			HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11944**	om/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	
Improper Input Validation	05-06-2019	10	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11945**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/122
N/A	05-06-2019	6.8	A remote credential disclosure vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11946**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/123
Use of Hard-coded Credentials	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11947**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/124
Improper Input	05-06-2019	9	A remote code execution vulnerability was identified in	https://support.hpe.c	A-HP-INTE-210619/125

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			HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11948**	om/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	10	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11949**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/126
Deserialization of Untrusted Data	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11950**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/127
Improper Neutralization of Special Elements in Output Used by a Downstream	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11951**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03	A-HP-INTE-210619/128

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
Component ('Injection')				930en_us	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11952**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/129
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11953**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/130
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11954**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/131

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 a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11955**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/132
Deserialization of Untrusted Data	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11956**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/133
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-06-2019	9.3	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11957**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/134
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11958**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	A-HP-INTE-210619/135

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
				hpesbhf03930en_us	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11959**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/136
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11960**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/137
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11961**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/138
Improper Neutralization of	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management	https://support.hpe.com/hpsc/d	A-HP-INTE-210619/139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Special Elements in Output Used by a Downstream Component ('Injection')			Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11962**	oc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11963**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/140
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11964**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/141
Improper Neutralization of Special	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than	https://support.hpe.com/hpsc/doc/public/	A-HP-INTE-210619/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			version 7.3 E0506P09. **CVE ID : CVE-2019-11965**	display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	
N/A	05-06-2019	9	A remote privilege escalation vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11966**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/143
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11967**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/144
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11968**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/145
Improper	05-06-2019	9	A remote code execution	https://su	A-HP-INTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')			vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11969**	pport.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	210619/146
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-06-2019	9	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11970**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/147
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-06-2019	9	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11971**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/148
Improper Neutralization of Special Elements used in	05-06-2019	9	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11972**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en	A-HP-INTE-210619/149

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
an SQL Command ('SQL Injection')				_US&docId=emr_na-hpesbhf03930en_us	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-06-2019	9	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11973**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/150
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-06-2019	9	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11974**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/151
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-06-2019	9	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11975**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/152
Improper Neutraliz	05-06-2019	9	A SQL injection code execution vulnerability was identified in	https://support.hpe.c	A-HP-INTE-210619/153

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
ation of Special Elements used in an SQL Command ('SQL Injection')			HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11976**	om/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-06-2019	9	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11977**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/154
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-06-2019	9	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11978**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/155
Improper Neutralization of Special Elements used in an SQL Command ('SQL	05-06-2019	9	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11979**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03	A-HP-INTE-210619/156

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')				930en_us	
Improper Input Validation	05-06-2019	9	A remote code exection vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11980**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/157
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-06-2019	9	A SQL injection code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11984**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/158
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-11985**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/159
Improper Neutralization of Special Elements	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09.	https://support.hpe.com/hpsc/doc/public/display?do	A-HP-INTE-210619/160

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
used in a Command ('Command Injection')			**CVE ID : CVE-2019-11986**	cLocale=en_US&docId=emr_na-hpesbhf03930en_us	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5346**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/161
Improper Input Validation	05-06-2019	10	A remote authentication bypass vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5347**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/162
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5348**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/163
Improper	05-06-2019	9	A remote code execution	https://su	A-HP-INTE-

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 was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5349**	pport.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	210619/164
Deserialization of Untrusted Data	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5350**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/165
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5351**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/166
Improper Neutralization of Special Elements in Output Used by a Downstre	05-06-2019	10	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5352**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	A-HP-INTE-210619/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
am Component ('Injection')				hpesbhf03930en_us	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5353**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/168
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5354**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/169
Improper Input Validation	05-06-2019	7.8	A remote denial of service vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5355**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/170

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-06-2019	10	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5356**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/171
Unrestricted Upload of File with Dangerous Type	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5357**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/172
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-06-2019	10	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5358**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/173
Improper Neutralization of Special Elements used in a Comman	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5359**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId	A-HP-INTE-210619/174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d ('Command Injection')				=emr_na-hpesbhf03930en_us	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5360**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/175
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5361**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/176
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5362**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/177
Improper	05-06-2019	9	A remote code execution	https://su	A-HP-INTE-

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 was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5363**	pport.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	210619/178
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5364**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/179
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5365**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/180
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5366**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/181
Improper	05-06-2019	10	A remote code execution	https://su	A-HP-INTE-

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
Authentication			vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5367**	pport.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	210619/182
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5368**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/183
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5369**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/184
Improper Neutralization of Special Elements used in a Command ('Command Injection'	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5370**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/185

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 a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5371**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/186
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5372**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/187
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5373**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/188
Improper Neutralization of	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management	https://support.hpe.com/hpsc/d	A-HP-INTE-210619/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5374**	oc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5375**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/190
Improper Input Validation	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5376**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/191
Improper Neutralization of Special Elements in Output Used by a Downstream	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5377**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03	A-HP-INTE-210619/192

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
Component ('Injection')				930en_us	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5378**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/193
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5379**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/194
Improper Neutralization of Special Elements in Output Used by a Downstream Compone	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5380**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/195

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
nt ('Injection')					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5381**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/196
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5382**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/197
Improper Neutralization of Special Elements in Output Used by a Downstream Component	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5383**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/198

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')					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5384**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/199
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5385**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/200
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injectio	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5386**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n')					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	10	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5387**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/202
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5388**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/203
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-06-2019	9	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5389**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/204

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 a Command ('Command Injection')	05-06-2019	10	A remote command injection vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5390**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/205
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-06-2019	10	A stack buffer overflow vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5391**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/206
Information Exposure	05-06-2019	5	A disclosure of information vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5392**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03930en_us	A-HP-INTE-210619/207
Improper Neutralization of Special Elements in Output Used by a Downstre	05-06-2019	6.8	A remote code execution vulnerability was identified in HPE Intelligent Management Center (IMC) PLAT earlier than version 7.3 E0506P09. **CVE ID : CVE-2019-5393**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	A-HP-INTE-210619/208

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
am Component ('Injection')				hpesbhf03930en_us	
Huawei					
pcmanager					
N/A	06-06-2019	9.3	There is a privilege escalation vulnerability in Huawei PCManager versions earlier than PCManager 9.0.1.50. The attacker can tricking a user to install and run a malicious application to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege. **CVE ID : CVE-2019-5241**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190109-01-pcmanager-en	A-HUA-PCMA-210619/209
Improper Input Validation	06-06-2019	9.3	There is a code execution vulnerability in Huawei PCManager versions earlier than PCManager 9.0.1.50. The attacker can tricking a user to install and run a malicious application to exploit this vulnerability. Successful exploitation may cause the attacker to execute malicious code and read/write memory. **CVE ID : CVE-2019-5242**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190109-01-pcmanager-en	A-HUA-PCMA-210619/210
hisuite					
Untrusted Search Path	13-06-2019	4.6	HiSuite 9.1.0.300 versions and earlier contains a DLL hijacking vulnerability. This vulnerability exists due to some DLL file is loaded by HiSuite improperly. And it allows an attacker to load this DLL file of the attacker's choosing that could execute	N/A	A-HUA-HISU-210619/211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code. **CVE ID : CVE-2019-5245**		
IBM					
control_desk					
Information Exposure	05-06-2019	2.1	IBM Maximo Asset Management 7.6 could allow a physical user of the system to obtain sensitive information from a previous user of the same machine. IBM X-Force ID: 156311. **CVE ID : CVE-2019-4048**	https://www.ibm.com/support/docview.wss?uid=ibm10880147	A-IBM-CONT-210619/212
Unrestricted Upload of File with Dangerous Type	05-06-2019	4	IBM Maximo Asset Management 7.6 Work Centers' application does not validate file type upon upload, allowing attackers to upload malicious files. IBM X-Force ID: 156565. **CVE ID : CVE-2019-4056**	https://www.ibm.com/support/docview.wss?uid=ibm10880149	A-IBM-CONT-210619/213
maximo_asset_management					
Information Exposure	05-06-2019	2.1	IBM Maximo Asset Management 7.6 could allow a physical user of the system to obtain sensitive information from a previous user of the same machine. IBM X-Force ID: 156311. **CVE ID : CVE-2019-4048**	https://www.ibm.com/support/docview.wss?uid=ibm10880147	A-IBM-MAXI-210619/214
Unrestricted Upload of File with Dangerous Type	05-06-2019	4	IBM Maximo Asset Management 7.6 Work Centers' application does not validate file type upon upload, allowing attackers to upload malicious files. IBM X-Force ID: 156565. **CVE ID : CVE-2019-4056**	https://www.ibm.com/support/docview.wss?uid=ibm10880149	A-IBM-MAXI-210619/215
maximo_for_aviation					
Information	05-06-2019	2.1	IBM Maximo Asset Management 7.6 could allow a physical user of the system to obtain sensitive	https://www.ibm.com/support	A-IBM-MAXI-

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			information from a previous user of the same machine. IBM X-Force ID: 156311. **CVE ID : CVE-2019-4048**	/docview.wss?uid=ibm10880147	210619/216
Unrestricted Upload of File with Dangerous Type	05-06-2019	4	IBM Maximo Asset Management 7.6 Work Centers' application does not validate file type upon upload, allowing attackers to upload malicious files. IBM X-Force ID: 156565. **CVE ID : CVE-2019-4056**	https://www.ibm.com/support/docview.wss?uid=ibm10880149	A-IBM-MAXI-210619/217
maximo_for_life_sciences					
Information Exposure	05-06-2019	2.1	IBM Maximo Asset Management 7.6 could allow a physical user of the system to obtain sensitive information from a previous user of the same machine. IBM X-Force ID: 156311. **CVE ID : CVE-2019-4048**	https://www.ibm.com/support/docview.wss?uid=ibm10880147	A-IBM-MAXI-210619/218
Unrestricted Upload of File with Dangerous Type	05-06-2019	4	IBM Maximo Asset Management 7.6 Work Centers' application does not validate file type upon upload, allowing attackers to upload malicious files. IBM X-Force ID: 156565. **CVE ID : CVE-2019-4056**	https://www.ibm.com/support/docview.wss?uid=ibm10880149	A-IBM-MAXI-210619/219
maximo_for_nuclear_power					
Information Exposure	05-06-2019	2.1	IBM Maximo Asset Management 7.6 could allow a physical user of the system to obtain sensitive information from a previous user of the same machine. IBM X-Force ID: 156311. **CVE ID : CVE-2019-4048**	https://www.ibm.com/support/docview.wss?uid=ibm10880147	A-IBM-MAXI-210619/220
Unrestricted Upload of	05-06-2019	4	IBM Maximo Asset Management 7.6 Work Centers' application does not validate file type upon	https://www.ibm.com/support	A-IBM-MAXI-210619/221

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
File with Dangerous Type			upload, allowing attackers to upload malicious files. IBM X-Force ID: 156565. **CVE ID : CVE-2019-4056**	/docview.wss?uid=ibm10880149	
maximo_for_oil_and_gas					
Information Exposure	05-06-2019	2.1	IBM Maximo Asset Management 7.6 could allow a physical user of the system to obtain sensitive information from a previous user of the same machine. IBM X-Force ID: 156311. **CVE ID : CVE-2019-4048**	https://www.ibm.com/support/docview.wss?uid=ibm10880147	A-IBM-MAXI-210619/222
Unrestricted Upload of File with Dangerous Type	05-06-2019	4	IBM Maximo Asset Management 7.6 Work Centers' application does not validate file type upon upload, allowing attackers to upload malicious files. IBM X-Force ID: 156565. **CVE ID : CVE-2019-4056**	https://www.ibm.com/support/docview.wss?uid=ibm10880149	A-IBM-MAXI-210619/223
maximo_for_transportation					
Information Exposure	05-06-2019	2.1	IBM Maximo Asset Management 7.6 could allow a physical user of the system to obtain sensitive information from a previous user of the same machine. IBM X-Force ID: 156311. **CVE ID : CVE-2019-4048**	https://www.ibm.com/support/docview.wss?uid=ibm10880147	A-IBM-MAXI-210619/224
Unrestricted Upload of File with Dangerous Type	05-06-2019	4	IBM Maximo Asset Management 7.6 Work Centers' application does not validate file type upon upload, allowing attackers to upload malicious files. IBM X-Force ID: 156565. **CVE ID : CVE-2019-4056**	https://www.ibm.com/support/docview.wss?uid=ibm10880149	A-IBM-MAXI-210619/225
maximo_for_utilities					
Information	05-06-2019	2.1	IBM Maximo Asset Management 7.6 could allow a physical user of	https://www.ibm.co	A-IBM-MAXI-

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			the system to obtain sensitive information from a previous user of the same machine. IBM X-Force ID: 156311. **CVE ID : CVE-2019-4048**	m/support/docview.wss?uid=ibm10880147	210619/226
Unrestricted Upload of File with Dangerous Type	05-06-2019	4	IBM Maximo Asset Management 7.6 Work Centers' application does not validate file type upon upload, allowing attackers to upload malicious files. IBM X-Force ID: 156565. **CVE ID : CVE-2019-4056**	https://www.ibm.com/support/docview.wss?uid=ibm10880149	A-IBM-MAXI-210619/227
smartcloud_control_desk					
Information Exposure	05-06-2019	2.1	IBM Maximo Asset Management 7.6 could allow a physical user of the system to obtain sensitive information from a previous user of the same machine. IBM X-Force ID: 156311. **CVE ID : CVE-2019-4048**	https://www.ibm.com/support/docview.wss?uid=ibm10880147	A-IBM-SMAR-210619/228
Unrestricted Upload of File with Dangerous Type	05-06-2019	4	IBM Maximo Asset Management 7.6 Work Centers' application does not validate file type upon upload, allowing attackers to upload malicious files. IBM X-Force ID: 156565. **CVE ID : CVE-2019-4056**	https://www.ibm.com/support/docview.wss?uid=ibm10880149	A-IBM-SMAR-210619/229
tivoli_integration_composer					
Information Exposure	05-06-2019	2.1	IBM Maximo Asset Management 7.6 could allow a physical user of the system to obtain sensitive information from a previous user of the same machine. IBM X-Force ID: 156311. **CVE ID : CVE-2019-4048**	https://www.ibm.com/support/docview.wss?uid=ibm10880147	A-IBM-TIVO-210619/230
Unrestricted	05-06-2019	4	IBM Maximo Asset Management 7.6 Work Centers' application	https://www.ibm.co	A-IBM-TIVO-210619/231

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
Upload of File with Dangerous Type			does not validate file type upon upload, allowing attackers to upload malicious files. IBM X-Force ID: 156565. **CVE ID : CVE-2019-4056**	m/support/docview.wss?uid=ibm10880149	
intelligent_operations_center					
Improper Input Validation	07-06-2019	6.5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 could allow an authenciated user to create arbitrary users which could cause ID management issues and result in code execution. IBM X-Force ID: 157011. **CVE ID : CVE-2019-4066**	https://www.ibm.com/support/docview.wss?uid=ibm10879381	A-IBM-INTE-210619/232
Information Exposure	07-06-2019	5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 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: 157012. **CVE ID : CVE-2019-4067**	https://www.ibm.com/support/docview.wss?uid=ibm10880213	A-IBM-INTE-210619/233
Information Exposure	07-06-2019	5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 is vulnerable to user enumeration, allowing an attacker to brute force into the system. IBM X-Force ID: 157013. **CVE ID : CVE-2019-4068**	https://www.ibm.com/support/docview.wss?uid=ibm10880229	A-IBM-INTE-210619/234
Unrestricted Upload of File with Dangerous Type	07-06-2019	6.5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 does not properly validate file types, allowing an attacker to upload malicious content. IBM X-Force ID: 157014. **CVE ID : CVE-2019-4069**	https://www.ibm.com/support/docview.wss?uid=ibm10879953	A-IBM-INTE-210619/235

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')	07-06-2019	3.5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 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: 157015. **CVE ID : CVE-2019-4070**	https://www.ibm.com/support/docview.wss?uid=ibm10879943	A-IBM-INTE-210619/236
intelligent_operations_center_for_emergency_management					
Improper Input Validation	07-06-2019	6.5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 could allow an authenciated user to create arbitrary users which could cause ID management issues and result in code execution. IBM X-Force ID: 157011. **CVE ID : CVE-2019-4066**	https://www.ibm.com/support/docview.wss?uid=ibm10879381	A-IBM-INTE-210619/237
Information Exposure	07-06-2019	5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 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: 157012. **CVE ID : CVE-2019-4067**	https://www.ibm.com/support/docview.wss?uid=ibm10880213	A-IBM-INTE-210619/238
Information Exposure	07-06-2019	5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 is vulnerable to user enumeration, allowing an attacker to brute force into the system. IBM X-Force ID: 157013. **CVE ID : CVE-2019-4068**	https://www.ibm.com/support/docview.wss?uid=ibm10880229	A-IBM-INTE-210619/239
Unrestric	07-06-2019	6.5	IBM Intelligent Operations Center	https://w	A-IBM-INTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ted Upload of File with Dangerous Type			(IOC) 5.1.0 through 5.2.0 does not properly validate file types, allowing an attacker to upload malicious content. IBM X-Force ID: 157014. **CVE ID : CVE-2019-4069**	ww.ibm.com/support/docview.wss?uid=ibm10879953	210619/240
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-06-2019	3.5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 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: 157015. **CVE ID : CVE-2019-4070**	https://www.ibm.com/support/docview.wss?uid=ibm10879943	A-IBM-INTE-210619/241
water_operations_for_waternamics					
Improper Input Validation	07-06-2019	6.5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 could allow an authenciated user to create arbitrary users which could cause ID management issues and result in code execution. IBM X-Force ID: 157011. **CVE ID : CVE-2019-4066**	https://www.ibm.com/support/docview.wss?uid=ibm10879381	A-IBM-WATE-210619/242
Information Exposure	07-06-2019	5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 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: 157012. **CVE ID : CVE-2019-4067**	https://www.ibm.com/support/docview.wss?uid=ibm10880213	A-IBM-WATE-210619/243
Information	07-06-2019	5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 is	https://www.ibm.co	A-IBM-WATE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			vulnerable to user enumeration, allowing an attacker to brute force into the system. IBM X-Force ID: 157013. **CVE ID : CVE-2019-4068**	m/support/docview.wss?uid=ibm10880229	210619/244
Unrestricted Upload of File with Dangerous Type	07-06-2019	6.5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 does not properly validate file types, allowing an attacker to upload malicious content. IBM X-Force ID: 157014. **CVE ID : CVE-2019-4069**	https://www.ibm.com/support/docview.wss?uid=ibm10879953	A-IBM-WATE-210619/245
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-06-2019	3.5	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 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: 157015. **CVE ID : CVE-2019-4070**	https://www.ibm.com/support/docview.wss?uid=ibm10879943	A-IBM-WATE-210619/246
security_information_queue					
Improper Input Validation	06-06-2019	4.3	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, and 1.0.2 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 159226. **CVE ID : CVE-2019-4217**	https://www.ibm.com/support/docview.wss?uid=ibm10886051	A-IBM-SECU-210619/247
Information	06-06-2019	2.1	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, and 1.0.2	https://www.ibm.co	A-IBM-SECU-210619/248

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			allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 159227. **CVE ID : CVE-2019-4218**	m/support/docview.wss?uid=ibm10886061	
Information Exposure	06-06-2019	5	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, and 1.0.2 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 159228. **CVE ID : CVE-2019-4219**	https://www.ibm.com/support/docview.wss?uid=ibm10886065	A-IBM-SECU-210619/249
Information Exposure	06-06-2019	2.1	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, and 1.0.2 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 158660. **CVE ID : CVE-2019-4161**	https://www.ibm.com/support/docview.wss?uid=ibm10885959	A-IBM-SECU-210619/250
Improper Input Validation	06-06-2019	5	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, and 1.0.2 is missing the HTTP Strict Transport Security header. Users can navigate by mistake to the unencrypted version of the web application or accept invalid certificates. This leads to sensitive data being sent unencrypted over the wire. IBM X-Force ID: 158661. **CVE ID : CVE-2019-4162**	https://www.ibm.com/support/docview.wss?uid=ibm10885963	A-IBM-SECU-210619/251
watson_knowledge_catalog					
Use of Hard-coded Credentia	05-06-2019	2.1	IBM InfoSphere Information Server 11.7.1.0 stores a common hard coded encryption key that could be used to decrypt	https://www.ibm.com/support/docview.	A-IBM-WATS-210619/252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ls			sensitive information. IBM X-Force ID: 159229. **CVE ID : CVE-2019-4220**	wss?uid=ibm10881197	
infosphere_information_analyzer					
Information Exposure	06-06-2019	4	IBM InfoSphere Information Server 11.5 and 11.7 is affected by an information disclosure vulnerability. Sensitive information in an error message may be used to conduct further attacks against the system. IBM X-Force ID: 159945. **CVE ID : CVE-2019-4257**	https://www.ibm.com/support/docview.wss?uid=ibm10882478	A-IBM-INFO-210619/253
infosphere_information_governance_catalog					
Information Exposure	06-06-2019	4	IBM InfoSphere Information Server 11.5 and 11.7 is affected by an information disclosure vulnerability. Sensitive information in an error message may be used to conduct further attacks against the system. IBM X-Force ID: 159945. **CVE ID : CVE-2019-4257**	https://www.ibm.com/support/docview.wss?uid=ibm10882478	A-IBM-INFO-210619/254
infosphere_information_server					
N/A	05-06-2019	5.4	IBM InfoSphere Information Server 11.7.1 containers are vulnerable to privilege escalation due to an insecurely configured component. IBM X-Force ID: 158975. **CVE ID : CVE-2019-4185**	https://www.ibm.com/support/docview.wss?uid=ibm10882626	A-IBM-INFO-210619/255
infosphere_information_server_on_cloud					
Use of Hard-coded Credentials	05-06-2019	2.1	IBM InfoSphere Information Server 11.7.1.0 stores a common hard coded encryption key that could be used to decrypt sensitive information. IBM X-	https://www.ibm.com/support/docview.wss?uid=ib	A-IBM-INFO-210619/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Force ID: 159229. **CVE ID : CVE-2019-4220**	m10881197	
Information Exposure	06-06-2019	4	IBM InfoSphere Information Server 11.5 and 11.7 is affected by an information disclosure vulnerability. Sensitive information in an error message may be used to conduct further attacks against the system. IBM X-Force ID: 159945. **CVE ID : CVE-2019-4257**	https://www.ibm.com/support/docview.wss?uid=ibm10882478	A-IBM-INFO-210619/257
N/A	05-06-2019	5.4	IBM InfoSphere Information Server 11.7.1 containers are vulnerable to privilege escalation due to an insecurely configured component. IBM X-Force ID: 158975. **CVE ID : CVE-2019-4185**	https://www.ibm.com/support/docview.wss?uid=ibm10882626	A-IBM-INFO-210619/258
Icewarp					
mail_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-06-2019	5	IceWarp Mail Server through 10.4.4 is prone to a local file inclusion vulnerability via webmail/calendar/minimizer/index.php?style=..%5c directory traversal. **CVE ID : CVE-2019-12593**	N/A	A-ICE-MAIL-210619/259
Ikiwiki					
ikiwiki					
Server-Side Request Forgery	05-06-2019	5	ikiwiki before 3.20170111.1 and 3.2018x and 3.2019x before 3.20190226 allows SSRF via the aggregate plugin. The impact also includes reading local files via	N/A	A-IKI-IKIW-210619/260

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
(SSRF)			file: URIs. **CVE ID : CVE-2019-9187**		
Intel					
turbo_boost_max_technology_3.0					
N/A	13-06-2019	4.4	Improper permissions in the installer for Intel(R) Turbo Boost Max Technology 3.0 driver version 1.0.0.1035 and before may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2019-0164**	N/A	A-INT-TURB-210619/261
open_cloud_integrity_tehnology					
N/A	13-06-2019	3.6	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0179**	N/A	A-INT-OPEN-210619/262
N/A	13-06-2019	3.6	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0180**	N/A	A-INT-OPEN-210619/263
Improper Input Validation	13-06-2019	4.6	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0181**	N/A	A-INT-OPEN-210619/264
Improper Limitation of a	13-06-2019	2.1	Insufficient password protection in the attestation database for Open CIT may allow an	N/A	A-INT-OPEN-210619/265

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
Pathname to a Restricted Directory ('Path Traversal')			authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0182**		
Information Exposure	13-06-2019	2.1	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0183**	N/A	A-INT-OPEN-210619/266
N/A	13-06-2019	3.6	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-11092**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00248.html	A-INT-OPEN-210619/267
N/A	13-06-2019	3.6	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0175**	N/A	A-INT-OPEN-210619/268
Improper Input Validation	13-06-2019	3.6	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access.	N/A	A-INT-OPEN-210619/269

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-2019-0177		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-06-2019	3.3	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0178**	N/A	A-INT-OPEN-210619/270
openattestation					
N/A	13-06-2019	3.6	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0179**	N/A	A-INT-OPEN-210619/271
N/A	13-06-2019	3.6	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0180**	N/A	A-INT-OPEN-210619/272
Improper Input Validation	13-06-2019	4.6	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0181**	N/A	A-INT-OPEN-210619/273
Improper Limitatio	13-06-2019	2.1	Insufficient password protection in the attestation database for	N/A	A-INT-OPEN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of a Pathnam e to a Restricte d Directory ('Path Traversal ')			Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0182**		210619/274
Informati on Exposure	13-06-2019	2.1	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0183**	N/A	A-INT-OPEN-210619/275
N/A	13-06-2019	3.6	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-11092**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00248.html	A-INT-OPEN-210619/276
N/A	13-06-2019	3.6	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0175**	N/A	A-INT-OPEN-210619/277
Improper Input Validatio n	13-06-2019	3.6	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via	N/A	A-INT-OPEN-210619/278

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
			local access. **CVE ID : CVE-2019-0177**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	13-06-2019	3.3	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access. **CVE ID : CVE-2019-0178**	N/A	A-INT-OPEN-210619/279
investment_mlm_project					
investment_mlm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-06-2019	3.5	An issue was discovered in PHP Scripts Mall Investment MLM Software 2.0.2. Stored XSS was found in the the My Profile Section. This is due to lack of sanitization in the Edit Name section. **CVE ID : CVE-2019-7552**	N/A	A-INV-INVE-210619/280
Ipswitch					
ws_ftp_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path	11-06-2019	5	A Directory Traversal issue was discovered in SSHServerAPI.dll in Progress ipswitch WS_FTP Server 2018 before 8.6.1. An attacker can supply a string using special patterns via the SCP protocol to disclose WS_FTP usernames as well as filenames.	https://docs.ipswitch.com/WS_FTP_Server2018/ReleaseNotes/index.htm#49242.htm	A-IPS-WS_F-210619/281

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
Traversal ')			**CVE ID : CVE-2019-12143**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal ')	11-06-2019	7.5	An issue was discovered in SSHServerAPI.dll in Progress ipswitch WS_FTP Server 2018 before 8.6.1. Attackers have the ability to abuse a path traversal vulnerability using the SCP protocol. Attackers who leverage this flaw could also obtain remote code execution by crafting a payload that abuses the SITE command feature. **CVE ID : CVE-2019-12144**	https://docs.ipswitch.com/WS_FTP_Server2018/ReleaseNotes/index.htm#49242.htm	A-IPS-WS_F-210619/282
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal ')	11-06-2019	5	A Directory Traversal issue was discovered in SSHServerAPI.dll in Progress ipswitch WS_FTP Server 2018 before 8.6.1. An attacker can supply a string using special patterns via the SCP protocol to disclose path names on the host operating system. **CVE ID : CVE-2019-12145**	https://docs.ipswitch.com/WS_FTP_Server2018/ReleaseNotes/index.htm#49242.htm	A-IPS-WS_F-210619/283
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal ')	11-06-2019	6.4	A Directory Traversal issue was discovered in SSHServerAPI.dll in Progress ipswitch WS_FTP Server 2018 before 8.6.1. Attackers have the ability to abuse a flaw in the SCP listener by crafting strings using specific patterns to write files and create directories outside of their authorized directory. **CVE ID : CVE-2019-12146**	https://docs.ipswitch.com/WS_FTP_Server2018/ReleaseNotes/index.htm#49242.htm	A-IPS-WS_F-210619/284
istio					
istio					

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 Access Control	05-06-2019	5.4	Istio 1.1.x through 1.1.6 has Incorrect Access Control. **CVE ID : CVE-2019-12243**	https://istio.io/blog/2019/cve-2019-12243/	A-IST-ISTI-210619/285
ivanti					
landesk_management_suite					
N/A	03-06-2019	5	Improper access control and open directories in Ivanti LANDESK Management Suite (LDMS, aka Endpoint Manager) 10.0.1.168 Service Update 5 may lead to remote disclosure of administrator passwords. **CVE ID : CVE-2019-12373**	N/A	A-IVA-LAND-210619/286
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-06-2019	6.8	A SQL Injection vulnerability exists in Ivanti LANDESK Management Suite (LDMS, aka Endpoint Manager) 10.0.1.168 Service Update 5 due to improper username sanitization in the Basic Authentication implementation in core/provisioning.secure/ProvisioningSecure.asmx in Provisioning.Secure.dll. **CVE ID : CVE-2019-12374**	N/A	A-IVA-LAND-210619/287
Improper Input Validation	03-06-2019	7.5	Open directories in Ivanti LANDESK Management Suite (LDMS, aka Endpoint Manager) 10.0.1.168 Service Update 5 may lead to remote information disclosure and arbitrary code execution. **CVE ID : CVE-2019-12375**	N/A	A-IVA-LAND-210619/288
Use of Hard-coded	03-06-2019	3.5	Use of a hard-coded encryption key in Ivanti LANDESK Management Suite (LDMS, aka	N/A	A-IVA-LAND-210619/289

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			Endpoint Manager) 10.0.1.168 Service Update 5 may lead to full managed endpoint compromise by an authenticated user with read privileges. **CVE ID : CVE-2019-12376**		
Unrestricted Upload of File with Dangerous Type	03-06-2019	7.5	A vulnerable upl/async_upload.asp web API endpoint in Ivanti LANDESK Management Suite (LDMS, aka Endpoint Manager) 10.0.1.168 Service Update 5 allows arbitrary file upload, which may lead to arbitrary remote code execution. **CVE ID : CVE-2019-12377**	N/A	A-IVA-LAND-210619/290
Jenkins					
electricflow					
Cross-Site Request Forgery (CSRF)	11-06-2019	4.3	A cross-site request forgery vulnerability in Jenkins ElectricFlow Plugin 1.1.5 and earlier in Configuration#doTestConnection allowed attackers to connect to an attacker-specified URL using attacker-specified credentials. **CVE ID : CVE-2019-10331**	N/A	A-JEN-ELEC-210619/291
N/A	11-06-2019	4.3	A missing permission check in Jenkins ElectricFlow Plugin 1.1.5 and earlier in Configuration#doTestConnection allowed users with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials. **CVE ID : CVE-2019-10332**	N/A	A-JEN-ELEC-210619/292
Information Exposure	11-06-2019	4	Missing permission checks in Jenkins ElectricFlow Plugin 1.1.5 and earlier in various HTTP	N/A	A-JEN-ELEC-210619/293

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
			endpoints allowed users with Overall/Read access to obtain information about the Jenkins ElectricFlow Plugin configuration and configuration of connected ElectricFlow instances. **CVE ID : CVE-2019-10333**		
Improper Certificate Validation	11-06-2019	5.8	Jenkins ElectricFlow Plugin 1.1.5 and earlier disabled SSL/TLS and hostname verification globally for the Jenkins master JVM when MultipartUtility.java is used to upload files. **CVE ID : CVE-2019-10334**	N/A	A-JEN-ELEC-210619/294
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-06-2019	3.5	A stored cross site scripting vulnerability in Jenkins ElectricFlow Plugin 1.1.5 and earlier allowed attackers able to configure jobs in Jenkins or control the output of the ElectricFlow API to inject arbitrary HTML and JavaScript in the plugin-provided output on build status pages. **CVE ID : CVE-2019-10335**	N/A	A-JEN-ELEC-210619/295
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-06-2019	4.3	A reflected cross site scripting vulnerability in Jenkins ElectricFlow Plugin 1.1.6 and earlier allowed attackers able to control the output of the ElectricFlow API to inject arbitrary HTML and JavaScript in job configuration forms containing post-build steps provided by this plugin. **CVE ID : CVE-2019-10336**	N/A	A-JEN-ELEC-210619/296
jx_resources					
Cross-	11-06-2019	6.8	A cross-site request forgery	N/A	A-JEN-JX_R-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Site Request Forgery (CSRF)			vulnerability in Jenkins JX Resources Plugin 1.0.36 and earlier in GlobalPluginConfiguration#doValidateClient allowed attackers to have Jenkins connect to an attacker-specified Kubernetes server, potentially leaking credentials. **CVE ID : CVE-2019-10338**		210619/297
N/A	11-06-2019	4	A missing permission check in Jenkins JX Resources Plugin 1.0.36 and earlier in GlobalPluginConfiguration#doValidateClient allowed users with Overall/Read access to have Jenkins connect to an attacker-specified Kubernetes server, potentially leaking credentials. **CVE ID : CVE-2019-10339**	N/A	A-JEN-JX_R-210619/298
token_macro					
Improper Restriction of XML External Entity Reference ('XXE')	11-06-2019	5	An XML external entities (XXE) vulnerability in Jenkins Token Macro Plugin 2.7 and earlier allowed attackers able to control a the content of the input file for the "XML" macro to have Jenkins resolve external entities, resulting in the extraction of secrets from the Jenkins agent, server-side request forgery, or denial-of-service attacks. **CVE ID : CVE-2019-10337**	N/A	A-JEN-TOKE-210619/299
Joomla					
Joomla!					
Improper Access Control	11-06-2019	4	An issue was discovered in Joomla! before 3.9.7. The update server URL of com_joomlaupdate	N/A	A-JOO-JOOM-210619/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can be manipulated by non Super-Admin users. **CVE ID : CVE-2019-12764**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	11-06-2019	7.5	An issue was discovered in Joomla! before 3.9.7. The CSV export of com_actionslogs is vulnerable to CSV injection. **CVE ID : CVE-2019-12765**	N/A	A-JOO-JOOM-210619/301
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-06-2019	4.3	An issue was discovered in Joomla! before 3.9.7. The subform fieldtype does not sufficiently filter or validate input of subfields. This leads to XSS attack vectors. **CVE ID : CVE-2019-12766**	N/A	A-JOO-JOOM-210619/302
Libreswan					
libreswan					
Improper Input Validation	12-06-2019	3.5	The Libreswan Project has found a vulnerability in the processing of IKEv1 informational exchange packets which are encrypted and integrity protected using the established IKE SA encryption and integrity keys, but as a receiver, the integrity check value was not verified. This issue affects versions before 3.29.	N/A	A-LIB-LIBR-210619/303

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-2019-10155		
Liferay					
liferay_portal					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2019	2.6	In Liferay Portal before 7.1 CE GA4, an XSS vulnerability exists in the SimpleCaptcha API when custom code passes unsanitized input into the "url" parameter of the JSP taglib call <liferay-ui:captcha url="<%= url %>" /> or <liferay-captcha:captcha url="<%= url %>" />. Liferay Portal out-of-the-box behavior with no customizations is not vulnerable. **CVE ID : CVE-2019-6588**	https://dev.liferay.com/web/community-security-team/known-vulnerabilities/liferay-portal-71/-/asset_publisher/7v4O7y85hZMo/content/cst-7130-multiple-xss-vulnerabilities-in-7-1-ce-ga3	A-LIF-LIFE-210619/304
Malwarebytes					
antimalware					
Improper Input Validation	03-06-2019	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Malwarebytes Antimalware 3.6.1.2711. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page. There is an issue with the way the product handles URIs within certain schemes. The product does not warn the user that a dangerous navigation is about to	N/A	A-MAL-ANTI-210619/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			take place. Because special characters in the URI are not sanitized, this could lead to the execution of arbitrary commands. An attacker can leverage this vulnerability to execute code in the context of the current user at medium integrity. Was ZDI-CAN-7162. **CVE ID : CVE-2019-6739**		
Microfocus					
solutions_business_manager					
URL Redirection to Untrusted Site ('Open Redirect')	07-06-2019	5.8	Micro Focus Solution Business Manager versions prior to 11.4.2 is susceptible to open redirect. **CVE ID : CVE-2019-3477**	http://help.serena.com/doc_center/sbm/ver11_4_2/sbm_release_notes.htm	A-MIC-SOLU-210619/306
service_manager					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-06-2019	9	Remote unauthorized command execution and unauthorized disclosure of information 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. This vulnerability could allow Remote unauthorized command execution and unauthorized disclosure of information. **CVE ID : CVE-2019-11646**	N/A	A-MIC-SERV-210619/307
Microsoft					
lync_server					
Improper Input Validation	12-06-2019	7.1	A denial of service vulnerability exists in Skype for Business, aka 'Skype for Business and Lync Server Denial of Service	N/A	A-MIC-LYNC-210619/308

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-2019-1029**		
office_web_apps					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1035. **CVE ID : CVE-2019-1034**	N/A	A-MIC-OFFI-210619/309
project_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	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'. This CVE ID is unique from CVE-2019-1031, CVE-2019-1032, CVE-2019-1036. **CVE ID : CVE-2019-1033**	N/A	A-MIC-PROJ-210619/310
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	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'. This CVE ID is unique from CVE-2019-1032, CVE-2019-1033, CVE-2019-1036. **CVE ID : CVE-2019-1031**	N/A	A-MIC-PROJ-210619/311
Improper Neutraliz	12-06-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when	N/A	A-MIC-PROJ-210619/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ation of Input During Web Page Generation ('Cross-site Scripting')			Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2019-1031, CVE-2019-1032, CVE-2019-1033. **CVE ID : CVE-2019-1036**		
chakracore					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052. **CVE ID : CVE-2019-0989**	N/A	A-MIC-CHAK-210619/313
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting Engine Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1023. **CVE ID : CVE-2019-0990**	N/A	A-MIC-CHAK-210619/314
Improper Restriction of Operations within the	12-06-2019	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	N/A	A-MIC-CHAK-210619/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0989, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052. **CVE ID : CVE-2019-0991**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052. **CVE ID : CVE-2019-0993**	N/A	A-MIC-CHAK-210619/316
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052. **CVE ID : CVE-2019-1003**	N/A	A-MIC-CHAK-210619/317
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting Engine Information	N/A	A-MIC-CHAK-210619/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0990. **CVE ID : CVE-2019-1023**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1051, CVE-2019-1052. **CVE ID : CVE-2019-1024**	N/A	A-MIC-CHAK-210619/319
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1052. **CVE ID : CVE-2019-1051**	N/A	A-MIC-CHAK-210619/320
Improper Restriction of Operations within the Bounds of a Memory	12-06-2019	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-2019-0989, CVE-2019-0991, CVE-	N/A	A-MIC-CHAK-210619/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051. **CVE ID : CVE-2019-1052**		
edge					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052. **CVE ID : CVE-2019-0989**	N/A	A-MIC-EDGE-210619/322
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting Engine Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1023. **CVE ID : CVE-2019-0990**	N/A	A-MIC-EDGE-210619/323
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0989, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024,	N/A	A-MIC-EDGE-210619/324

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
			CVE-2019-1051, CVE-2019-1052. **CVE ID : CVE-2019-0991**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0989, CVE-2019-0991, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052. **CVE ID : CVE-2019-0992**	N/A	A-MIC-EDGE-210619/325
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052. **CVE ID : CVE-2019-0993**	N/A	A-MIC-EDGE-210619/326
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1003, CVE-2019-1024,	N/A	A-MIC-EDGE-210619/327

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-2019-1051, CVE-2019-1052. **CVE ID : CVE-2019-1002**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1024, CVE-2019-1051, CVE-2019-1052. **CVE ID : CVE-2019-1003**	N/A	A-MIC-EDGE-210619/328
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting Engine Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0990. **CVE ID : CVE-2019-1023**	N/A	A-MIC-EDGE-210619/329
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1051, CVE-2019-1052. **CVE ID : CVE-2019-1024**	N/A	A-MIC-EDGE-210619/330

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	12-06-2019	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2019-1038**	N/A	A-MIC-EDGE-210619/331
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1052. **CVE ID : CVE-2019-1051**	N/A	A-MIC-EDGE-210619/332
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0989, CVE-2019-0991, CVE-2019-0992, CVE-2019-0993, CVE-2019-1002, CVE-2019-1003, CVE-2019-1024, CVE-2019-1051. **CVE ID : CVE-2019-1052**	N/A	A-MIC-EDGE-210619/333
N/A	12-06-2019	5.1	A security feature bypass vulnerability exists in Edge that allows for bypassing Mark of the Web Tagging (MOTW), aka	N/A	A-MIC-EDGE-210619/334

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
			'Microsoft Edge Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1054**		
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists when affected Microsoft browsers improperly handle objects in memory, aka 'Microsoft Browser Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1081**	N/A	A-MIC-EDGE-210619/335
office					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1035. **CVE ID : CVE-2019-1034**	N/A	A-MIC-OFFI-210619/336
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1034. **CVE ID : CVE-2019-1035**	N/A	A-MIC-OFFI-210619/337
office_365_proplus					
Improper Restriction of Operations within the Bounds	12-06-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is	N/A	A-MIC-OFFI-210619/338

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 a Memory Buffer			unique from CVE-2019-1035. **CVE ID : CVE-2019-1034**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1034. **CVE ID : CVE-2019-1035**	N/A	A-MIC-OFFI-210619/339
internet_explorer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0988, CVE-2019-1005, CVE-2019-1055, CVE-2019-1080. **CVE ID : CVE-2019-0920**	N/A	A-MIC-INTE-210619/340
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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'. This CVE ID is unique from CVE-2019-0920, CVE-2019-1005, CVE-2019-1055, CVE-2019-1080. **CVE ID : CVE-2019-0988**	N/A	A-MIC-INTE-210619/341
Improper Restriction of	12-06-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles objects	N/A	A-MIC-INTE-210619/342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0920, CVE-2019-0988, CVE-2019-1055, CVE-2019-1080. **CVE ID : CVE-2019-1005**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2019-1038**	N/A	A-MIC-INTE-210619/343
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0920, CVE-2019-0988, CVE-2019-1005, CVE-2019-1080. **CVE ID : CVE-2019-1055**	N/A	A-MIC-INTE-210619/344
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0920, CVE-2019-0988, CVE-2019-1005, CVE-2019-1055.	N/A	A-MIC-INTE-210619/345

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
			CVE ID : CVE-2019-1080		
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists when affected Microsoft browsers improperly handle objects in memory, aka 'Microsoft Browser Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1081**	N/A	A-MIC-INTE-210619/346
sharepoint_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	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'. This CVE ID is unique from CVE-2019-1031, CVE-2019-1033, CVE-2019-1036. **CVE ID : CVE-2019-1032**	N/A	A-MIC-SHAR-210619/347
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	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'. This CVE ID is unique from CVE-2019-1031, CVE-2019-1032, CVE-2019-1036. **CVE ID : CVE-2019-1033**	N/A	A-MIC-SHAR-210619/348
Improper Neutralization of Input During Web Page Generation ('Cross-	12-06-2019	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'. This CVE ID is	N/A	A-MIC-SHAR-210619/349

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
site Scripting')			unique from CVE-2019-1032, CVE-2019-1033, CVE-2019-1036. **CVE ID : CVE-2019-1031**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1035. **CVE ID : CVE-2019-1034**	N/A	A-MIC-SHAR-210619/350
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1034. **CVE ID : CVE-2019-1035**	N/A	A-MIC-SHAR-210619/351
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	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'. This CVE ID is unique from CVE-2019-1031, CVE-2019-1032, CVE-2019-1033. **CVE ID : CVE-2019-1036**	N/A	A-MIC-SHAR-210619/352
word					
Improper Restriction of Operatio	12-06-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in	N/A	A-MIC-WORD-210619/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ns within the Bounds of a Memory Buffer			memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1035. **CVE ID : CVE-2019-1034**		
sharepoint_enterprise_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	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'. This CVE ID is unique from CVE-2019-1031, CVE-2019-1033, CVE-2019-1036. **CVE ID : CVE-2019-1032**	N/A	A-MIC-SHAR-210619/354
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	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'. This CVE ID is unique from CVE-2019-1031, CVE-2019-1032, CVE-2019-1036. **CVE ID : CVE-2019-1033**	N/A	A-MIC-SHAR-210619/355
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'	12-06-2019	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'. This CVE ID is unique from CVE-2019-1032, CVE-2019-1033, CVE-2019-1036.	N/A	A-MIC-SHAR-210619/356

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
)			**CVE ID : CVE-2019-1031**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1035. **CVE ID : CVE-2019-1034**	N/A	A-MIC-SHAR-210619/357
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	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'. This CVE ID is unique from CVE-2019-1031, CVE-2019-1032, CVE-2019-1033. **CVE ID : CVE-2019-1036**	N/A	A-MIC-SHAR-210619/358
office_online_server					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1035. **CVE ID : CVE-2019-1034**	N/A	A-MIC-OFFI-210619/359
Improper Restriction of Operations within the	12-06-2019	9.3	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution	N/A	A-MIC-OFFI-210619/360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Vulnerability'. This CVE ID is unique from CVE-2019-1034. **CVE ID : CVE-2019-1035**		
sharepoint_foundation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	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'. This CVE ID is unique from CVE-2019-1031, CVE-2019-1032, CVE-2019-1036. **CVE ID : CVE-2019-1033**	N/A	A-MIC-SHAR-210619/361
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	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'. This CVE ID is unique from CVE-2019-1032, CVE-2019-1033, CVE-2019-1036. **CVE ID : CVE-2019-1031**	N/A	A-MIC-SHAR-210619/362
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	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'. This CVE ID is unique from CVE-2019-1031, CVE-2019-1032, CVE-2019-1033. **CVE ID : CVE-2019-1036**	N/A	A-MIC-SHAR-210619/363

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
Misp					
misp					
N/A	11-06-2019	6	An issue was discovered in MISP 2.4.108. Organization admins could reset credentials for site admins (organization admins have the inherent ability to reset passwords for all of their organization's users). This, however, could be abused in a situation where the host organization of an instance creates organization admins. An organization admin could set a password manually for the site admin or simply use the API key of the site admin to impersonate them. The potential for abuse only occurs when the host organization creates lower-privilege organization admins instead of the usual site admins. Also, only organization admins of the same organization as the site admin could abuse this. **CVE ID : CVE-2019-12794**	N/A	A-MIS-MISP-210619/364
Mybb					
mybb					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-06-2019	4.3	MyBB 1.8.19 has XSS in the resetpassword function. **CVE ID : CVE-2019-3578**	https://blog.mybb.com/2019/02/27/mybb-1-8-20-released-security-maintenance-release/	A-MYB-MYBB-210619/365

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
Information Exposure	06-06-2019	5	MyBB 1.8.19 allows remote attackers to obtain sensitive information because it discloses the username upon receiving a password-reset request that lacks the code parameter. **CVE ID : CVE-2019-3579**	https://blog.mybb.com/2019/02/27/mybb-1-8-20-released-security-maintenance-release/	A-MYB-MYBB-210619/366
Netgate					
Pfsense					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-06-2019	4.3	Apcupsd 0.3.91_5, as used in pfSense through 2.4.4-RELEASE-p3 and other products, has an XSS issue in apcupsd_status.php. **CVE ID : CVE-2019-12584**	N/A	A-NET-PFSE-210619/367
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-06-2019	7.5	Apcupsd 0.3.91_5, as used in pfSense through 2.4.4-RELEASE-p3 and other products, has an Arbitrary Command Execution issue in apcupsd_status.php. **CVE ID : CVE-2019-12585**	N/A	A-NET-PFSE-210619/368
northern					
cfengine					
N/A	06-06-2019	9	Northern.tech CFEngine Enterprise 3.12.1 has Insecure Permissions.	N/A	A-NOR-CFEN-210619/369

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
			CVE ID : CVE-2019-9929		
Omron					
network_configurator_for_devicenet_safety					
Untrusted Search Path	12-06-2019	6.8	The application (Network Configurator for DeviceNet Safety 3.41 and prior) searches for resources by means of an untrusted search path that could execute a malicious .dll file not under the application's direct control and outside the intended directories. **CVE ID : CVE-2019-10971**	N/A	A-OMR-NETW-210619/370
Openid					
ruby-openid					
Uncontrolled Resource Consumption	10-06-2019	10	Ruby OpenID (aka ruby-openid) through 2.8.0 has a remotely exploitable flaw. This library is used by Rails web applications to integrate with OpenID Providers. Severity can range from medium to critical, depending on how a web application developer chose to employ the ruby-openid library. Developers who based their OpenID integration heavily on the "example app" provided by the project are at highest risk. **CVE ID : CVE-2019-11027**	N/A	A-OPE-RUBY-210619/371
Openswan					
openswan					
Improper Input Validation	12-06-2019	3.5	The Libreswan Project has found a vulnerability in the processing of IKEv1 informational exchange packets which are encrypted and integrity protected using the established IKE SA encryption and integrity keys, but as a	N/A	A-OPE-OPEN-210619/372

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
			receiver, the integrity check value was not verified. This issue affects versions before 3.29. **CVE ID : CVE-2019-10155**		
Otrs					
otrs					
Information Exposure	03-06-2019	4	An issue was discovered in Open Ticket Request System (OTRS) 7.x before 7.0.5. An attacker who is logged into OTRS as an agent or a customer user can use the search result screens to disclose information from invalid system entities. Following is the list of affected entities: Custom Pages, FAQ Articles, Service Catalogue Items, ITSM Configuration Items. **CVE ID : CVE-2019-9753**	N/A	A-OTR-OTRS-210619/373
Panasonic					
control_fpwin_pro					
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-06-2019	6.8	Panasonic FPWIN Pro version 7.3.0.0 and prior allows attacker-created project files to be loaded by an authenticated user causing heap-based buffer overflows, which may lead to remote code execution. **CVE ID : CVE-2019-6530**	N/A	A-PAN-CONT-210619/374
Incorrect Type Conversion or Cast	07-06-2019	6.8	Panasonic FPWIN Pro version 7.3.0.0 and prior allows attacker-created project files to be loaded by an authenticated user triggering incompatible type errors because the resource does not have expected properties. This may lead to remote code	N/A	A-PAN-CONT-210619/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2019-6532**		
Papercut					
papercut_mf					
Improper Input Validation	06-06-2019	7.5	An unspecified vulnerability in the application server in PaperCut MF and NG versions 18.3.8 and earlier and versions 19.0.3 and earlier allows remote attackers to execute arbitrary code via an unspecified vector. **CVE ID : CVE-2019-12135**	https://www.papercut.com/products/mf/release-history/	A-PAP-PAPE-210619/376
papercut_ng					
Improper Input Validation	06-06-2019	7.5	An unspecified vulnerability in the application server in PaperCut MF and NG versions 18.3.8 and earlier and versions 19.0.3 and earlier allows remote attackers to execute arbitrary code via an unspecified vector. **CVE ID : CVE-2019-12135**	https://www.papercut.com/products/ng/release-history/	A-PAP-PAPE-210619/377
parso_project					
parso					
Deserialization of Untrusted Data	06-06-2019	6	A deserialization vulnerability exists in the way parso through 0.4.0 handles grammar parsing from the cache. Cache loading relies on pickle and, provided that an evil pickle can be written to a cache grammar file and that its parsing can be triggered, this flaw leads to Arbitrary Code Execution. **CVE ID : CVE-2019-12760**	N/A	A-PAR-PARS-210619/378
Photodex					
proshow_producer					

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	10-06-2019	6.8	An issue was discovered in Photodex ProShow Producer v9.0.3797 (an application that runs with Administrator privileges). It is possible to perform a buffer overflow via a crafted file. **CVE ID : CVE-2019-12788**	N/A	A-PHO-PROS-210619/379
Phpmyadmin					
phpmyadmin					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-06-2019	7.5	An issue was discovered in phpMyAdmin before 4.9.0.1. A vulnerability was reported where a specially crafted database name can be used to trigger an SQL injection attack through the designer feature. **CVE ID : CVE-2019-11768**	https://www.phpmyadmin.net/security/PMASA-2019-3/	A-PHP-PHPM-210619/380
Cross-Site Request Forgery (CSRF)	05-06-2019	4.3	An issue was discovered in phpMyAdmin before 4.9.0. A vulnerability was found that allows an attacker to trigger a CSRF attack against a phpMyAdmin user. The attacker can trick the user, for instance through a broken <img> tag pointing at the victim's phpMyAdmin database, and the attacker can potentially deliver a payload (such as a specific INSERT or DELETE statement) to the victim. **CVE ID : CVE-2019-12616**	https://www.phpmyadmin.net/security/PMASA-2019-4/	A-PHP-PHPM-210619/381
pippo					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pippo					
Uncontrolled Resource Consumption	12-06-2019	5	XML Entity Expansion (Billion Laughs Attack) on Pippo 1.12.0 results in Denial of Service.Entities are created recursively and large amounts of heap memory is taken. Eventually, the JVM process will run out of memory. Otherwise, if the OS does not bound the memory on that process, memory will continue to be exhausted and will affect other processes on the system. **CVE ID : CVE-2019-5442**	N/A	A-PIP-PIPP-210619/382
pivotal_software					
operations_manager					
Insufficient Session Expiration	06-06-2019	5.5	The Pivotal Ops Manager, 2.2.x versions prior to 2.2.23, 2.3.x versions prior to 2.3.16, 2.4.x versions prior to 2.4.11, and 2.5.x versions prior to 2.5.3, contain configuration that circumvents refresh token expiration. A remote authenticated user can gain access to a browser session that was supposed to have expired, and access Ops Manager resources. **CVE ID : CVE-2019-3790**	https://pivotal.io/security/cve-2019-3790	A-PIV-OPER-210619/383
primasystems					
flexair					
Improper Neutralization of Input During Web Page	05-06-2019	3.5	Prima Systems FlexAir devices allow Authenticated Stored XSS. **CVE ID : CVE-2019-7671**	N/A	A-PRI-FLEX-210619/384

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
Generation ('Cross-site Scripting')					
Use of Hard-coded Credentials	05-06-2019	7.5	Prima Systems FlexAir devices have Hard-coded Credentials. **CVE ID : CVE-2019-7672**	N/A	A-PRI-FLEX-210619/385
Unrestricted Upload of File with Dangerous Type	05-06-2019	9	On Prima Systems FlexAir devices through 2.4.9api3, an authenticated user can upload Python (.py) scripts and execute arbitrary code with root privileges. **CVE ID : CVE-2019-9189**	N/A	A-PRI-FLEX-210619/386
Progress					
fiddler					
N/A	03-06-2019	6.8	Telerik Fiddler v5.0.20182.28034 doesn't verify the hash of EnableLoopback.exe before running it, which could lead to code execution or local privilege escalation by replacing the original EnableLoopback.exe. **CVE ID : CVE-2019-12097**	N/A	A-PRO-FIDD-210619/387
Pulsesecure					
pulse_policy_secure					
Improper Access Control	03-06-2019	6.5	In Pulse Secure Pulse Connect Secure (PCS) before 8.1R15.1, 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4 and Pulse Policy Secure (PPS) before 5.1R15.1, 5.2 before 5.2R12.1, 5.3 before 5.3R15.1, 5.4 before 5.4R7.1, and 9.0 before 9.0R3.2, an authenticated	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101/	A-PUL-PULS-210619/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker (via the admin web interface) can exploit Incorrect Access Control to execute arbitrary code on the appliance. **CVE ID : CVE-2019-11509**		
pulse_connect_secure					
Improper Access Control	03-06-2019	6.5	In Pulse Secure Pulse Connect Secure (PCS) before 8.1R15.1, 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4 and Pulse Policy Secure (PPS) before 5.1R15.1, 5.2 before 5.2R12.1, 5.3 before 5.3R15.1, 5.4 before 5.4R7.1, and 9.0 before 9.0R3.2, an authenticated attacker (via the admin web interface) can exploit Incorrect Access Control to execute arbitrary code on the appliance. **CVE ID : CVE-2019-11509**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101/	A-PUL-PULS-210619/389
Pydio					
pydio					
Unrestricted Upload of File with Dangerous Type	05-06-2019	7.5	An issue was discovered in proxy.php in pydio-core in Pydio through 8.2.2. Through an unauthenticated request, it possible to evaluate malicious PHP code by placing it on the fourth line of a .php file, as demonstrated by a PoC.php created by the guest account, with execution via a proxy.php?hash=../../../../../var/lib/pydio/data/personal/guest/PoC.php request. This is related to plugins/action.share/src/Store/ShareStore.php. **CVE ID : CVE-2019-9642**	https://pydio.com/en/community/releases/pydio-core/pydio-core-pydio-enterprise-823-security-release	A-PYD-PYDI-210619/390

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
Python					
pyxdg					
XML Injection (aka Blind XPath Injection)	06-06-2019	5.1	A code injection issue was discovered in PyXDG before 0.26 via crafted Python code in a Category element of a Menu XML document in a .menu file. XDG_CONFIG_DIRS must be set up to trigger xdg.Menu.parse parsing within the directory containing this file. This is due to a lack of sanitization in xdg/Menu.py before an eval call. **CVE ID : CVE-2019-12761**	N/A	A-PYT-PYXD-210619/391
python					
N/A	07-06-2019	5	A security regression of CVE-2019-9636 was discovered in python since commit d537ab0ff9767ef024f26246899728f0116b1ec3 affecting versions 2.7, 3.5, 3.6, 3.7 and from v3.8.0a4 through v3.8.0b1, which still allows an attacker to exploit CVE-2019-9636 by abusing the user and password parts of a URL. When an application parses user-supplied URLs to store cookies, authentication credentials, or other kind of information, it is possible for an attacker to provide specially crafted URLs to make the application locate host-related information (e.g. cookies, authentication data) and send them to a different host than where it should, unlike if the URLs had been correctly parsed. The result of an attack may vary	N/A	A-PYT-PYTH-210619/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			based on the application. **CVE ID : CVE-2019-10160**		
Qemu					
qemu					
Information Exposure	03-06-2019	2.1	tcp_emu in slirp/tcp_subr.c (aka slirp/src/tcp_subr.c) in QEMU 3.0.0 uses uninitialized data in an snprintf call, leading to Information disclosure. **CVE ID : CVE-2019-9824**	N/A	A-QEM-QEMU-210619/393
Radare					
radare2					
Out-of-bounds Read	10-06-2019	6.8	In radare2 through 3.5.1, there is a heap-based buffer over-read in the r_egg_lang_parsechar function of egg_lang.c. This allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact because of missing length validation in libr/egg/egg.c. **CVE ID : CVE-2019-12790**	N/A	A-RAD-RADA-210619/394
rakuten					
viber					
Untrusted Search Path	02-06-2019	9.3	A vulnerability in Viber before 10.7.0 for Desktop (Windows) could allow an attacker to execute arbitrary commands on a targeted system. This vulnerability is due to unsafe search paths used by the application URI. An attacker could exploit this vulnerability by convincing a targeted user to follow a malicious link. Successful exploitation could cause the	N/A	A-RAK-VIBE-210619/395

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
			application to load libraries from the directory targeted by the URI link. The attacker could use this behavior to execute arbitrary commands on the system with the privileges of the targeted user, if the attacker can place a crafted library in a directory that is accessible to the vulnerable system. **CVE ID : CVE-2019-12569**		
rancher					
rancher					
Improper Input Validation	10-06-2019	4.3	A vulnerability exists in Rancher 2.1.4 in the login component, where the errorMsg parameter can be tampered to display arbitrary content, filtering tags but not special characters or symbols. There's no other limitation of the message, allowing malicious users to lure legitimate users to visit phishing sites with scare tactics, e.g., displaying a "This version of Rancher is outdated, please visit https://malicious.rancher.site/upgrading" message. **CVE ID : CVE-2019-11881**	https://github.com/rancher/rancher/issues/20216	A-RAN-RANC-210619/396
N/A	06-06-2019	4	In Rancher 1 and 2 through 2.2.3, unprivileged users (if allowed to deploy nodes) can gain admin access to the Rancher management plane because node driver options intentionally allow posting certain data to the cloud. The problem is that a user could choose to post a sensitive file such as /root/.kube/config or	https://forums.rancher.com/t/rancher-release-v2-2-4-addresses-rancher-cve-2019-12274-	A-RAN-RANC-210619/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/var/lib/rancher/management-state/cred/kubeconfig-system.yaml. **CVE ID : CVE-2019-12274**	and-cve-2019-12303/14466	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-06-2019	6.5	In Rancher 2 through 2.2.3, Project owners can inject additional fluentd configuration to read files or execute arbitrary commands inside the fluentd container. **CVE ID : CVE-2019-12303**	https://forums.rancher.com/t/rancher-release-v2-2-4-addresses-rancher-cve-2019-12274-and-cve-2019-12303/14466	A-RAN-RANC-210619/398
Redhat					
rkt					
Information Exposure	03-06-2019	6.9	rkt through version 1.30.0 does not isolate processes in containers that are run with `rkt enter`. Processes run with `rkt enter` are given all capabilities during stage 2 (the actual environment in which the applications run). Compromised containers could exploit this flaw to access host resources. **CVE ID : CVE-2019-10144**	N/A	A-RED-RKT-210619/399
Information Exposure	03-06-2019	6.9	rkt through version 1.30.0 does not isolate processes in containers that are run with `rkt enter`. Processes run with `rkt enter` do not have seccomp filtering during stage 2 (the actual environment in which the applications run). Compromised	N/A	A-RED-RKT-210619/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			containers could exploit this flaw to access host resources. **CVE ID : CVE-2019-10145**		
Information Exposure	03-06-2019	6.9	rkt through version 1.30.0 does not isolate processes in containers that are run with `rkt enter`. Processes run with `rkt enter` are not limited by cgroups during stage 2 (the actual environment in which the applications run). Compromised containers could exploit this flaw to access host resources. **CVE ID : CVE-2019-10147**	N/A	A-RED-RKT-210619/401
keycloak					
Improper Authentication	12-06-2019	2.1	It was found that Keycloak's Node.js adapter before version 4.8.3 did not properly verify the web token received from the server in its backchannel logout . An attacker with local access could use this to construct a malicious web token setting an NBF parameter that could prevent user access indefinitely. **CVE ID : CVE-2019-10157**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10157	A-RED-KEYC-210619/402
Improper Certificate Validation	12-06-2019	5.8	A vulnerability was found in keycloak before 6.0.2. The X.509 authenticator supports the verification of client certificates through the CRL, where the CRL list can be obtained from the URL provided in the certificate itself (CDP) or through the separately configured path. The CRL are often available over the network through unsecured protocols ('http' or 'ldap') and hence the caller should verify the signature	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3875	A-RED-KEYC-210619/403

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 possibly the certification path. Keycloak currently doesn't validate signatures on CRL, which can result in a possibility of various attacks like man-in-the-middle. **CVE ID : CVE-2019-3875**		
jboss_enterprise_application_platform					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	3.5	It was found that a SAMLRequest containing a script could be processed by Picketlink versions shipped in Jboss Application Platform 7.2.x and 7.1.x. An attacker could use this to send a malicious script to achieve cross-site scripting and obtain unauthorized information or conduct further attacks. **CVE ID : CVE-2019-3872**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3872	A-RED-JBOS-210619/404
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	6	It was found that Picketlink as shipped with Jboss Enterprise Application Platform 7.2 would accept an xinclude parameter in SAMLresponse XML. An attacker could use this flaw to send a URL to achieve cross-site scripting or possibly conduct further attacks. **CVE ID : CVE-2019-3873**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3873	A-RED-JBOS-210619/405
single_sign-on					
Improper Neutralization of Input During Web Page Generation ('Cross-	12-06-2019	3.5	It was found that a SAMLRequest containing a script could be processed by Picketlink versions shipped in Jboss Application Platform 7.2.x and 7.1.x. An attacker could use this to send a malicious script to achieve cross-site scripting and obtain	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3872	A-RED-SING-210619/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
site Scripting')			unauthorized information or conduct further attacks. **CVE ID : CVE-2019-3872**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	6	It was found that Picketlink as shipped with Jboss Enterprise Application Platform 7.2 would accept an xinclude parameter in SAMLresponse XML. An attacker could use this flaw to send a URL to achieve cross-site scripting or possibly conduct further attacks. **CVE ID : CVE-2019-3873**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3873	A-RED-SING-210619/407
Improper Certificate Validation	12-06-2019	5.8	A vulnerability was found in keycloak before 6.0.2. The X.509 authenticator supports the verification of client certificates through the CRL, where the CRL list can be obtained from the URL provided in the certificate itself (CDP) or through the separately configured path. The CRL are often available over the network through unsecured protocols ('http' or 'ldap') and hence the caller should verify the signature and possibly the certification path. Keycloak currently doesn't validate signatures on CRL, which can result in a possibility of various attacks like man-in-the-middle. **CVE ID : CVE-2019-3875**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3875	A-RED-SING-210619/408
openshift_container_platform					
Improper Authentication	12-06-2019	4.3	It was found that OpenShift Container Platform versions 3.6.x - 4.6.0 does not perform SSH Host Key checking when using ssh key	N/A	A-RED-OPEN-210619/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication during builds. An attacker, with the ability to redirect network traffic, could use this to alter the resulting build output. **CVE ID : CVE-2019-10150**		
openstack					
Improper Access Control	03-06-2019	6.8	An access-control flaw was found in the Octavia service when the cloud platform was deployed using Red Hat OpenStack Platform Director. An attacker could cause new amphorae to run based on any arbitrary image. This meant that a remote attacker could upload a new amphorae image and, if requested to spawn new amphorae, Octavia would then pick up the compromised image. **CVE ID : CVE-2019-3895**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3895	A-RED-OPEN-210619/410
undertow					
N/A	12-06-2019	5	A vulnerability was found in Undertow web server before 2.0.21. An information exposure of plain text credentials through log files because Connectors.executeRootHandler: 402 logs the HttpServerExchange object at ERROR level using UndertowLogger.REQUEST_LOGGER.undertowRequestFailed(t, exchange) **CVE ID : CVE-2019-3888**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3888	A-RED-UNDE-210619/411
Rubygems					
rubygems					
Improper Limitatio	06-06-2019	8.8	A Directory Traversal issue was discovered in RubyGems 2.7.6	N/A	A-RUB-RUBY-

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
n of a Pathnam e to a Restricte d Directory ('Path Traversal ')			and later through 3.0.2. Before making new directories or touching files (which now include path-checking code for symlinks), it would delete the target destination. If that destination was hidden behind a symlink, a malicious gem could delete arbitrary files on the user's machine, presuming the attacker could guess at paths. Given how frequently gem is run as sudo, and how predictable paths are on modern systems (/tmp, /usr, etc.), this could likely lead to data loss or an unusable system. **CVE ID : CVE-2019-8320**		210619/412
salesagility					
suitecrm					
Improper Neutraliz ation of Special Elements used in an SQL Comman d ('SQL Injection')	07-06-2019	7.5	SuiteCRM 7.8.x before 7.8.30, 7.10.x before 7.10.17, and 7.11.x before 7.11.5 allows SQL Injection (issue 1 of 3). **CVE ID : CVE-2019-12598**	https://do cs.suitecrm .com/admi n/releases /7.11.x/#_ 7_11_5	A-SAL-SUIT-210619/413
Improper Neutraliz ation of Special Elements used in an SQL Comman d ('SQL Injection'	07-06-2019	7.5	SuiteCRM 7.10.x before 7.10.17 and 7.11.x before 7.11.5 allows SQL Injection. **CVE ID : CVE-2019-12599**	https://do cs.suitecrm .com/admi n/releases /7.11.x/#_ 7_11_5	A-SAL-SUIT-210619/414

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')	07-06-2019	7.5	SuiteCRM 7.8.x before 7.8.30, 7.10.x before 7.10.17, and 7.11.x before 7.11.5 allows SQL Injection (issue 2 of 3). **CVE ID : CVE-2019-12600**	https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_5	A-SAL-SUIT-210619/415
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-06-2019	7.5	SuiteCRM 7.8.x before 7.8.30, 7.10.x before 7.10.17, and 7.11.x before 7.11.5 allows SQL Injection (issue 3 of 3). **CVE ID : CVE-2019-12601**	https://docs.suitecrm.com/admin/releases/7.11.x/#_7_11_5	A-SAL-SUIT-210619/416
SAP					
netweaver_process_integration					
Deserialization of Untrusted Data	12-06-2019	4.3	Java Server Pages (JSPs) provided by the SAP NetWeaver Process Integration (SAP_XIESR and SAP_XITOOL: 7.10 to 7.11, 7.20, 7.30, 7.31, 7.40, 7.50) do not restrict or incorrectly restrict frame objects or UI layers that belong to another application or domain, resulting in Clickjacking vulnerability. Successful exploitation of this vulnerability leads to unwanted modification of user's data. **CVE ID : CVE-2019-0305**	N/A	A-SAP-NETW-210619/417

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	12-06-2019	5	Several web pages provided SAP NetWeaver Process Integration (versions: SAP_XIESR: 7.10 to 7.11, 7.20, 7.30, 7.31, 7.40, 7.50 and SAP_XITOOL: 7.10 to 7.11, 7.30, 7.31, 7.40, 7.50) are not password protected. An attacker could access landscape information like host names, ports or other technical data in the absence of restrictive firewall and port settings. **CVE ID : CVE-2019-0312**	N/A	A-SAP-NETW-210619/418
Information Exposure	12-06-2019	5	Under certain conditions the PI Integration Builder Web UI of SAP NetWeaver Process Integration (versions: SAP_XIESR: 7.10 to 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, SAP_XITOOL: 7.10 to 7.11, 7.30, 7.31, 7.40, 7.50 and SAP_XIPCK 7.10 to 7.11, 7.20, 7.30) allows an attacker to access passwords used in FTP channels leading to information disclosure. **CVE ID : CVE-2019-0315**	N/A	A-SAP-NETW-210619/419
r/3_enterprise					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-06-2019	4.3	Automotive Dealer Portal in SAP R/3 Enterprise Application (versions: 600, 602, 603, 604, 605, 606, 616, 617) does not sufficiently encode user-controlled inputs, this makes it possible for an attacker to send unwanted scripts to the browser of the victim using unwanted input and execute malicious code there, resulting in Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2019-0311**	N/A	A-SAP-R/3_-210619/420

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
inventory_manager					
Improper Access Control	12-06-2019	4.3	SAP Work Manager, versions: 6.3, 6.4, 6.5 and SAP Inventory Manager, version 4.3, allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service. **CVE ID : CVE-2019-0314**	N/A	A-SAP-INVE-210619/421
solution_manager					
N/A	12-06-2019	2.7	Diagnostics Agent in Solution Manager, version 7.2, stores several credentials such as SLD user connection as well as Solman user communication in the SAP Secure Storage file which is not encrypted by default. By decoding these credentials, an attacker with admin privileges could gain access to the entire configuration, but no system sensitive information can be gained. **CVE ID : CVE-2019-0307**	N/A	A-SAP-SOLU-210619/422
e-commerce					
Improper Control of Generation of Code ('Code Injection')	12-06-2019	3.5	An authenticated attacker in SAP E-Commerce (Business-to-Consumer application), versions 7.3, 7.31, 7.32, 7.33, 7.54, can change the price of the product to zero and also checkout, by injecting an HTML code in the application that will be executed whenever the victim logs in to the application even on a different machine, leading to Code Injection. **CVE ID : CVE-2019-0308**	N/A	A-SAP-E-CO-210619/423

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
work_manager					
Improper Access Control	12-06-2019	4.3	SAP Work Manager, versions: 6.3, 6.4, 6.5 and SAP Inventory Manager, version 4.3, allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service. **CVE ID : CVE-2019-0314**	N/A	A-SAP-WORK-210619/424
advanced_business_application_programming_platform_kernel					
Improper Control of Generation of Code ('Code Injection')	12-06-2019	7.5	FTP Function of SAP NetWeaver AS ABAP Platform, versions- KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73, KERNEL 7.21, 7.45, 7.49, 7.53, 7.73, allows an attacker to inject code or specifically manipulated command that can be executed by the application. An attacker could thereby control the behaviour of the application. **CVE ID : CVE-2019-0304**	N/A	A-SAP-ADVA-210619/425
advanced_business_application_programming_platform_krnl64nuc					
Improper Control of Generation of Code ('Code Injection')	12-06-2019	7.5	FTP Function of SAP NetWeaver AS ABAP Platform, versions- KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73, KERNEL 7.21, 7.45, 7.49, 7.53, 7.73, allows an attacker to inject code or specifically manipulated command that can	N/A	A-SAP-ADVA-210619/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be executed by the application. An attacker could thereby control the behaviour of the application. **CVE ID : CVE-2019-0304**		
advanced_business_application_programming_platform_krnl64uc					
Improper Control of Generation of Code ('Code Injection')	12-06-2019	7.5	FTP Function of SAP NetWeaver AS ABAP Platform, versions- KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73, KERNEL 7.21, 7.45, 7.49, 7.53, 7.73, allows an attacker to inject code or specifically manipulated command that can be executed by the application. An attacker could thereby control the behaviour of the application. **CVE ID : CVE-2019-0304**	N/A	A-SAP-ADVA-210619/427
advanced_business_application_programming_platform_krnl32nuc					
Improper Control of Generation of Code ('Code Injection')	12-06-2019	7.5	FTP Function of SAP NetWeaver AS ABAP Platform, versions- KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73, KERNEL 7.21, 7.45, 7.49, 7.53, 7.73, allows an attacker to inject code or specifically manipulated command that can be executed by the application. An attacker could thereby control the behaviour of the application. **CVE ID : CVE-2019-0304**	N/A	A-SAP-ADVA-210619/428

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
advanced_business_application_programming_platform_krnl32uc					
Improper Control of Generation of Code ('Code Injection')	12-06-2019	7.5	FTP Function of SAP NetWeaver AS ABAP Platform, versions- KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73, KERNEL 7.21, 7.45, 7.49, 7.53, 7.73, allows an attacker to inject code or specifically manipulated command that can be executed by the application. An attacker could thereby control the behaviour of the application. **CVE ID : CVE-2019-0304**	N/A	A-SAP-ADVA-210619/429
hana_extended_application_services					
Information Exposure	12-06-2019	4	SAP HANA Extended Application Services (advanced model), version 1, allows authenticated low privileged XS Advanced Platform users such as SpaceAuditors to execute requests to obtain a complete list of SAP HANA user IDs and names. **CVE ID : CVE-2019-0306**	N/A	A-SAP-HANA-210619/430
securitycamera					
security_camera_cz					
Information Exposure	07-06-2019	5	The Security Camera CZ application through 1.6.8 for Android stores potentially sensitive recorded video in external data storage, which is readable by any application. **CVE ID : CVE-2019-12763**	N/A	A-SEC-SECU-210619/431
Southrivertech					

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
titan_ftp_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-06-2019	4	A Directory Traversal issue was discovered in the Web GUI in Titan FTP Server 2019 Build 3505. When an authenticated user attempts to preview an uploaded file (through PreviewHandler.ashx) by using a \..\..\ technique, arbitrary files can be loaded in the server response outside the root directory. **CVE ID : CVE-2019-10009**	N/A	A-SOU-TITA-210619/432
Strongswan					
strongswan					
Improper Input Validation	12-06-2019	3.5	The Libreswan Project has found a vulnerability in the processing of IKEv1 informational exchange packets which are encrypted and integrity protected using the established IKE SA encryption and integrity keys, but as a receiver, the integrity check value was not verified. This issue affects versions before 3.29. **CVE ID : CVE-2019-10155**	N/A	A-STR-STRO-210619/433
Sweetscape					
010_editor					
Improper Input Validation	05-06-2019	7.5	In SweetScape 010 Editor 9.0.1, improper validation of arguments in the internal implementation of the StrCat function (provided by the scripting engine) allows an attacker to overwrite arbitrary memory, which could lead to code execution. **CVE ID : CVE-2019-12553**	https://www.sweetscape.com/010editor/release_notes.html	A-SWE-010_-210619/434

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	05-06-2019	5	In SweetScape 010 Editor 9.0.1, improper validation of arguments in the internal implementation of the WSubStr function (provided by the scripting engine) allows an attacker to cause a denial of service by crashing the application. **CVE ID : CVE-2019-12554**	https://www.sweetscape.com/010editor/release_notes.html	A-SWE-010_-210619/435
Improper Input Validation	05-06-2019	5	In SweetScape 010 Editor 9.0.1, improper validation of arguments in the internal implementation of the SubStr function (provided by the scripting engine) allows an attacker to cause a denial of service by crashing the application. **CVE ID : CVE-2019-12555**	https://www.sweetscape.com/010editor/release_notes.html	A-SWE-010_-210619/436
thinstation_project					
thinstation					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-06-2019	7.5	Command injection is possible in ThinStation through 6.1.1 via shell metacharacters after the cgi-bin/CdControl.cgi action= substring, or after the cgi-bin/VolControl.cgi OK= substring. **CVE ID : CVE-2019-12771**	N/A	A-THI-THIN-210619/437
titanhq					
spamtitan					
Improper Neutralization of Special	05-06-2019	8.5	In TitanHQ SpamTitan through 7.03, a vulnerability exists in the spam rule update function. Updates are downloaded over	https://www.spamtitan.com/category/spa	A-TIT-SPAM-210619/438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			HTTP, including scripts which are subsequently executed with root permissions. An attacker with a privileged network position is trivially able to inject arbitrary commands. **CVE ID : CVE-2019-6800**	mtitan-news/	
tuxera					
ntfs-3g					
Integer Underflow (Wrap or Wraparound)	05-06-2019	4.4	An integer underflow issue exists in ntfs-3g 2017.3.23. A local attacker could potentially exploit this by running /bin/ntfs-3g with specially crafted arguments from a specially crafted directory to cause a heap buffer overflow, resulting in a crash or the ability to execute arbitrary code. In installations where /bin/ntfs-3g is a setuid-root binary, this could lead to a local escalation of privileges. **CVE ID : CVE-2019-9755**	N/A	A-TUX-NTFS-210619/439
twistedmatrix					
twisted					
Improper Input Validation	10-06-2019	4.3	In Twisted before 19.2.1, twisted.web did not validate or sanitize URIs or HTTP methods, allowing an attacker to inject invalid characters such as CRLF. **CVE ID : CVE-2019-12387**	https://twistedmatrix.com/pipermail/twisted-python/2019-June/032352.html	A-TWI-TWIS-210619/440
tzumi					
klic_lock					

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	11-06-2019	4.3	An authentication bypass in website post requests in the Tzumi Electronics Klic Lock application 1.0.9 for mobile devices allows attackers to access resources (that are not otherwise accessible without proper authentication) via capture-replay. Physically proximate attackers can use this information to unlock unauthorized Tzumi Electronics Klic Smart Padlock Model 5686 Firmware 6.2. **CVE ID : CVE-2019-11334**	N/A	A-TZU-KLIC-210619/441
veronalabs					
wp_statistics					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-06-2019	3.5	The WP Statistics plugin through 12.6.5 for Wordpress has stored XSS in includes/class-wp-statistics-pages.php. This is related to an account with the Editor role creating a post with a title that contains JavaScript, to attack an admin user. **CVE ID : CVE-2019-12566**	N/A	A-VER-WP_S-210619/442
vfront					
vfront					
Improper Neutralization of Input During Web Page Generation ('Cross-site	03-06-2019	4.3	VFront 0.99.5 has stored XSS via the admin/sync_reg_tab.php azzera parameter, which is mishandled during admin/error_log.php rendering. **CVE ID : CVE-2019-9838**	N/A	A-VFR-VFRO-210619/443

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
Scripting')					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-06-2019	4.3	VFront 0.99.5 has Reflected XSS via the admin/menu_registri.php descrizione_g parameter or the admin/sync_reg_tab.php azzera parameter. **CVE ID : CVE-2019-9839**	N/A	A-VFR-VFRO-210619/444
Videolan					
vlc_media_player					
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-06-2019	4.3	A Buffer Overflow in VLC Media Player < 3.0.7 causes a crash which can possibly be further developed into a remote code execution exploit. **CVE ID : CVE-2019-5439**	N/A	A-VID-VLC_-210619/445
VIM					
vim					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'	05-06-2019	9.3	getchar.c in Vim before 8.1.1365 and Neovim before 0.3.6 allows remote attackers to execute arbitrary OS commands via the :source! command in a modeline, as demonstrated by execute in Vim, and assert_fails or nvim_input in Neovim. **CVE ID : CVE-2019-12735**	N/A	A-VIM-VIM-210619/446

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
)					
Vmware					
tools					
Out-of-bounds Read	06-06-2019	3.6	VMware Tools for Windows update addresses an out of bounds read vulnerability in vm3dmp driver which is installed with vmtools in Windows guest machines. This issue is present in versions 10.2.x and 10.3.x prior to 10.3.10. A local attacker with non-administrative access to a Windows guest with VMware Tools installed may be able to leak kernel information or create a denial of service attack on the same Windows guest machine. **CVE ID : CVE-2019-5522**	https://www.vmware.com/security/advisories/VMSA-2019-0009.html	A-VMW-TOOL-210619/447
workstation					
Use After Free	06-06-2019	7.2	VMware Workstation (15.x before 15.1.0) contains a use-after-free vulnerability in the Advanced Linux Sound Architecture (ALSA) backend. A malicious user with normal user privileges on the guest machine may exploit this issue in conjunction with other issues to execute code on the Linux host where Workstation is installed. **CVE ID : CVE-2019-5525**	https://www.vmware.com/security/advisories/VMSA-2019-0009.html	A-VMW-WORK-210619/448
Wampserver					
wampserver					
Cross-Site Request Forgery (CSRF)	10-06-2019	5.8	WampServer before 3.1.9 has CSRF in add_vhost.php because the synchronizer pattern implemented as remediation of CVE-2018-8817 was incomplete.	N/A	A-WAM-WAMP-210619/449

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
			An attacker could add/delete any vhosts without the consent of the owner. **CVE ID : CVE-2019-11517**		
workday					
workday					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-06-2019	6.5	CSV Injection (aka Excel Macro Injection or Formula Injection) exists in the export feature in Workday through 32 via a value (provided by a low-privileged user in a contact form field) that is mishandled in a CSV export. **CVE ID : CVE-2019-12134**	N/A	A-WOR-WORK-210619/450
wpgraphql					
wpgraphql					
Missing Authentication for Critical Function	10-06-2019	7.5	The WPGraphQL 0.2.3 plugin for WordPress allows remote attackers to register a new user with admin privileges, whenever new user registrations are allowed. This is related to the registerUser mutation. **CVE ID : CVE-2019-9879**	N/A	A-WPG-WPGR-210619/451
Missing Authentication for Critical Function	10-06-2019	6.4	An issue was discovered in the WPGraphQL 0.2.3 plugin for WordPress. By querying the 'users' RootQuery, it is possible, for an unauthenticated attacker, to retrieve all WordPress users details such as email address, role, and username. **CVE ID : CVE-2019-9880**	N/A	A-WPG-WPGR-210619/452

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
Missing Authentication for Critical Function	10-06-2019	5	The createComment mutation in the WPGraphQL 0.2.3 plugin for WordPress allows unauthenticated users to post comments on any article, even when 'allow comment' is disabled. **CVE ID : CVE-2019-9881**	N/A	A-WPG-WPGR-210619/453
x-cart					
x-cart					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-06-2019	4.3	X-Cart V5 is vulnerable to XSS via the CategoryFilter2 parameter. **CVE ID : CVE-2019-7220**	N/A	A-X-C-X-CA-210619/454
yubico					
pam-u2f					
Information Exposure	04-06-2019	5	Yubico pam-u2f 1.0.7 attempts parsing of the configured authfile (default $HOME/.config/Yubico/u2f_keys) as root (unless openasuser was enabled), and does not properly verify that the path lacks symlinks pointing to other files on the system owned by root. If the debug option is enabled in the PAM configuration, part of the file contents of a symlink target will be logged, possibly revealing sensitive information. **CVE ID : CVE-2019-12209**	https://github.com/Yubico/pam-u2f/commit/7db3386fcdb454e33a3ea30dcfb8e8960d4c3aa3	A-YUB-PAM--210619/455

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	04-06-2019	5.5	In Yubico pam-u2f 1.0.7, when configured with debug and a custom debug log file is set using debug_file, that file descriptor is not closed when a new process is spawned. This leads to the file descriptor being inherited into the child process; the child process can then read from and write to it. This can leak sensitive information and also, if written to, be used to fill the disk or plant misinformation. **CVE ID : CVE-2019-12210**	https://github.com/Yubico/pam-u2f/commit/18b1914e32b74ff52000f10e97067e841e5fff62	A-YUB-PAM-210619/456
Zohocorp					
manageengine_servicedesk_plus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-06-2019	4.3	An issue was discovered in Zoho ManageEngine ServiceDesk Plus 9.3. There is XSS via the SiteLookup.do search field. **CVE ID : CVE-2019-12538**	N/A	A-ZOH-MANA-210619/457
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-06-2019	4.3	An issue was discovered in Zoho ManageEngine ServiceDesk Plus 9.3. There is XSS via the SolutionSearch.do searchText parameter. **CVE ID : CVE-2019-12541**	N/A	A-ZOH-MANA-210619/458
Improper	05-06-2019	4.3	An issue was discovered in Zoho	N/A	A-ZOH-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			ManageEngine ServiceDesk Plus 9.3. There is XSS via the SearchN.do userConfigID parameter. **CVE ID : CVE-2019-12542**		MANA-210619/459
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-06-2019	4.3	An issue was discovered in Zoho ManageEngine ServiceDesk Plus 9.3. There is XSS via the PurchaseRequest.do serviceRequestId parameter. **CVE ID : CVE-2019-12543**	N/A	A-ZOH-MANA-210619/460
manageengine_netflow_analyzer					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-06-2019	7.5	A SQL injection vulnerability in /client/api/json/v2/nfareports/compareReport in Zoho ManageEngine NetFlow Analyzer 12.3 allows attackers to execute arbitrary SQL commands via the DeviceID parameter. **CVE ID : CVE-2019-12196**	N/A	A-ZOH-MANA-210619/461
Operating System					
anviz					
m3_firmware					
Improper Access Control	06-06-2019	7.5	Anviz Global M3 Outdoor RFID Access Control executes any command received from any	N/A	O-ANV-M3_F-210619/462

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
			source. No authentication/encryption is done. Attackers can fully interact with the device: for example, send the "open door" command, download the users list (which includes RFID codes and passcodes in cleartext), or update/create users. The same attack can be executed on a local network and over the internet (if the device is exposed on a public IP address). **CVE ID : CVE-2019-11523**		
Canonical					
ubuntu_linux					
Use After Free	11-06-2019	5	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly. **CVE ID : CVE-2019-0196**	N/A	O-CAN-UBUN-210619/463
N/A	11-06-2019	5	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them. **CVE ID : CVE-2019-0220**	N/A	O-CAN-UBUN-210619/464

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	11-06-2019	3.6	dbus before 1.10.28, 1.12.x before 1.12.16, and 1.13.x before 1.13.12, as used in DBusServer in Canonical Upstart in Ubuntu 14.04 (and in some, less common, uses of dbus-daemon), allows cookie spoofing because of symlink mishandling in the reference implementation of DBUS_COOKIE_SHA1 in the libdbus library. (This only affects the DBUS_COOKIE_SHA1 authentication mechanism.) A malicious client with write access to its own home directory could manipulate a ~/.dbus-keyrings symlink to cause a DBusServer with a different uid to read and write in unintended locations. In the worst case, this could result in the DBusServer reusing a cookie that is known to the malicious client, and treating that cookie as evidence that a subsequent client connection came from an attacker-chosen uid, allowing authentication bypass. **CVE ID : CVE-2019-12749**	N/A	O-CAN-UBUN-210619/465
Cisco					
ios_xr_firmware					
Improper Authorization	05-06-2019	5.5	A vulnerability in the Secure Shell (SSH) authentication function of Cisco IOS XR Software could allow an authenticated, remote attacker to successfully log in to an affected device using two distinct usernames. The vulnerability is due to a logic error that may occur when	N/A	O-CIS-IOS_-210619/466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certain sequences of actions are processed during an SSH login event on the affected device. An attacker could exploit this vulnerability by initiating an SSH session to the device with a specific sequence that presents the two usernames. A successful exploit could result in logging data misrepresentation, user enumeration, or, in certain circumstances, a command authorization bypass. See the Details section for more information. **CVE ID : CVE-2019-1842**		
Debian					
debian_linux					
Use After Free	11-06-2019	5	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly. **CVE ID : CVE-2019-0196**	N/A	O-DEB-DEBI-210619/467
N/A	11-06-2019	5	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.	N/A	O-DEB-DEBI-210619/468

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-2019-0220		
Dlink					
dir-818lw_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-06-2019	6.5	An issue was discovered on D-Link DIR-818LW devices from 2.05.B03 to 2.06B01 BETA. There is a command injection in HNAP1 SetWanSettings via an XML injection of the value of the IPAddress key. **CVE ID : CVE-2019-12786**	N/A	O-DLI-DIR--210619/469
XML Injection (aka Blind XPath Injection)	10-06-2019	6.5	An issue was discovered on D-Link DIR-818LW devices from 2.05.B03 to 2.06B01 BETA. There is a command injection in HNAP1 SetWanSettings via an XML injection of the value of the Gateway key. **CVE ID : CVE-2019-12787**	N/A	O-DLI-DIR--210619/470
enttec					
datagate_mk2_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-06-2019	4.3	A number of stored XSS vulnerabilities have been identified in the web configuration feature in ENTTEC Datagate Mk2 70044_update_05032019-482 that could allow an unauthenticated threat actor to inject malicious code directly into the application. This affects, for example, the Profile Description field in JSON data to the Profile Editor.	N/A	O-ENT-DATA-210619/471

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-2019-12774		
Improper Access Control	07-06-2019	9	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They allow high-privileged root access by www-data via sudo without requiring appropriate access control. (Furthermore, the user account that controls the web application service is granted full access to run any system commands with elevated privilege, without the need for password authentication. Should vulnerabilities be identified and exploited within the web application, it may be possible for a threat actor to create or run high-privileged binaries or executables that are available within the operating system of the device.) **CVE ID : CVE-2019-12775**	N/A	O-ENT-DATA-210619/472
Use of Hard-coded Credentials	07-06-2019	10	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They include a hard-coded SSH backdoor for remote SSH and SCP access as the root user. A command in the relocate and relocate_revB scripts copies the hardcoded key to the root user's authorized_keys file, enabling anyone with the associated private key to gain remote root access to all affected products.	N/A	O-ENT-DATA-210619/473

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-2019-12776		
N/A	07-06-2019	7.2	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They replace secure and protected directory permissions (set as default by the underlying operating system) with highly insecure read, write, and execute directory permissions for all users. By default, /usr/local and all of its subdirectories should have permissions set to only allow non-privileged users to read and execute from the tree structure, and to deny users from creating or editing files in this location. The ENTTEC firmware startup script permits all users to read, write, and execute (rwxrwxrwx) from the /usr, /usr/local, /usr/local/dmxis, and /usr/local/bin/ directories. **CVE ID : CVE-2019-12777**	N/A	O-ENT-DATA-210619/474
e-streamer_mk2_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-06-2019	4.3	A number of stored XSS vulnerabilities have been identified in the web configuration feature in ENTTEC Datagate Mk2 70044_update_05032019-482 that could allow an unauthenticated threat actor to inject malicious code directly into the application. This affects, for example, the Profile Description field in JSON data to the Profile Editor.	N/A	O-ENT-E-ST-210619/475

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
			CVE ID : CVE-2019-12774		
Improper Access Control	07-06-2019	9	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They allow high-privileged root access by www-data via sudo without requiring appropriate access control. (Furthermore, the user account that controls the web application service is granted full access to run any system commands with elevated privilege, without the need for password authentication. Should vulnerabilities be identified and exploited within the web application, it may be possible for a threat actor to create or run high-privileged binaries or executables that are available within the operating system of the device.) **CVE ID : CVE-2019-12775**	N/A	O-ENT-E-ST-210619/476
Use of Hard-coded Credentials	07-06-2019	10	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They include a hard-coded SSH backdoor for remote SSH and SCP access as the root user. A command in the relocate and relocate_revB scripts copies the hardcoded key to the root user's authorized_keys file, enabling anyone with the associated private key to gain remote root access to all affected products.	N/A	O-ENT-E-ST-210619/477

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-2019-12776		
N/A	07-06-2019	7.2	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They replace secure and protected directory permissions (set as default by the underlying operating system) with highly insecure read, write, and execute directory permissions for all users. By default, /usr/local and all of its subdirectories should have permissions set to only allow non-privileged users to read and execute from the tree structure, and to deny users from creating or editing files in this location. The ENTTEC firmware startup script permits all users to read, write, and execute (rwxrwxrwx) from the /usr, /usr/local, /usr/local/dmxis, and /usr/local/bin/ directories. **CVE ID : CVE-2019-12777**	N/A	O-ENT-E-ST-210619/478
pixelator_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-06-2019	4.3	A number of stored XSS vulnerabilities have been identified in the web configuration feature in ENTTEC Datagate Mk2 70044_update_05032019-482 that could allow an unauthenticated threat actor to inject malicious code directly into the application. This affects, for example, the Profile Description field in JSON data to the Profile Editor.	N/A	O-ENT-PIXE-210619/479

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-2019-12774		
Improper Access Control	07-06-2019	9	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They allow high-privileged root access by www-data via sudo without requiring appropriate access control. (Furthermore, the user account that controls the web application service is granted full access to run any system commands with elevated privilege, without the need for password authentication. Should vulnerabilities be identified and exploited within the web application, it may be possible for a threat actor to create or run high-privileged binaries or executables that are available within the operating system of the device.) **CVE ID : CVE-2019-12775**	N/A	O-ENT-PIXE-210619/480
Use of Hard-coded Credentials	07-06-2019	10	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They include a hard-coded SSH backdoor for remote SSH and SCP access as the root user. A command in the relocate and relocate_revB scripts copies the hardcoded key to the root user's authorized_keys file, enabling anyone with the associated private key to gain remote root access to all affected products.	N/A	O-ENT-PIXE-210619/481

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
			CVE ID : CVE-2019-12776		
N/A	07-06-2019	7.2	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They replace secure and protected directory permissions (set as default by the underlying operating system) with highly insecure read, write, and execute directory permissions for all users. By default, /usr/local and all of its subdirectories should have permissions set to only allow non-privileged users to read and execute from the tree structure, and to deny users from creating or editing files in this location. The ENTTEC firmware startup script permits all users to read, write, and execute (rwxrwxrwx) from the /usr, /usr/local, /usr/local/dmxis, and /usr/local/bin/ directories. **CVE ID : CVE-2019-12777**	N/A	O-ENT-PIXE-210619/482
storm_24_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-06-2019	4.3	A number of stored XSS vulnerabilities have been identified in the web configuration feature in ENTTEC Datagate Mk2 70044_update_05032019-482 that could allow an unauthenticated threat actor to inject malicious code directly into the application. This affects, for example, the Profile Description field in JSON data to the Profile Editor.	N/A	O-ENT-STOR-210619/483

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-2019-12774		
Improper Access Control	07-06-2019	9	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They allow high-privileged root access by www-data via sudo without requiring appropriate access control. (Furthermore, the user account that controls the web application service is granted full access to run any system commands with elevated privilege, without the need for password authentication. Should vulnerabilities be identified and exploited within the web application, it may be possible for a threat actor to create or run high-privileged binaries or executables that are available within the operating system of the device.) **CVE ID : CVE-2019-12775**	N/A	O-ENT-STOR-210619/484
Use of Hard-coded Credentials	07-06-2019	10	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They include a hard-coded SSH backdoor for remote SSH and SCP access as the root user. A command in the relocate and relocate_revB scripts copies the hardcoded key to the root user's authorized_keys file, enabling anyone with the associated private key to gain remote root access to all affected products.	N/A	O-ENT-STOR-210619/485

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-2019-12776		
N/A	07-06-2019	7.2	An issue was discovered on the ENTTEC Datagate MK2, Storm 24, Pixelator, and E-Streamer MK2 with firmware 70044_update_05032019-482. They replace secure and protected directory permissions (set as default by the underlying operating system) with highly insecure read, write, and execute directory permissions for all users. By default, /usr/local and all of its subdirectories should have permissions set to only allow non-privileged users to read and execute from the tree structure, and to deny users from creating or editing files in this location. The ENTTEC firmware startup script permits all users to read, write, and execute (rwxrwxrwx) from the /usr, /usr/local, /usr/local/dmxis, and /usr/local/bin/ directories. **CVE ID : CVE-2019-12777**	N/A	O-ENT-STOR-210619/486
Exagrid					
backup_appliance_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-06-2019	5	ExaGrid appliances with firmware version v4.8.1.1044.P50 have a /monitor/data/Upgrade/ directory traversal vulnerability, which allows remote attackers to view and retrieve verbose logging information. Files within this directory were observed to contain sensitive run-time information, including Base64 encoded 'support' credentials,	N/A	O-EXA-BACK-210619/487

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
			leading to administrative access of the device. **CVE ID : CVE-2019-12310**		
Fedoraproject					
fedora					
N/A	11-06-2019	5	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them. **CVE ID : CVE-2019-0220**	N/A	O-FED-FEDO-210619/488
Improper Input Validation	12-06-2019	3.5	The Libreswan Project has found a vulnerability in the processing of IKEv1 informational exchange packets which are encrypted and integrity protected using the established IKE SA encryption and integrity keys, but as a receiver, the integrity check value was not verified. This issue affects versions before 3.29. **CVE ID : CVE-2019-10155**	N/A	O-FED-FEDO-210619/489
Fortinet					
fortios					
Improper Neutralization of Input During Web Page Generation ('Cross-	04-06-2019	4.3	A reflected Cross-Site-Scripting (XSS) vulnerability in Fortinet FortiOS 5.2.0 to 6.0.4 under SSL VPN web portal may allow an attacker to execute unauthorized malicious script code via the "param" parameter of the error process HTTP requests.	https://fortiguard.com/advisory/FG-IR-19-034	O-FOR-FORT-210619/490

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
site Scripting')			**CVE ID : CVE-2019-5586**		
Improper Input Validation	04-06-2019	4	Lack of root file system integrity checking in Fortinet FortiOS VM application images all versions below 6.0.5 may allow attacker to implant malicious programs into the installing image by reassembling the image through specific methods. **CVE ID : CVE-2019-5587**	https://fortiguard.com/advisory/FG-IR-19-017	O-FOR-FORT-210619/491
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-06-2019	4.3	A reflected Cross-Site-Scripting (XSS) vulnerability in Fortinet FortiOS 6.0.0 to 6.0.4 under SSL VPN web portal may allow an attacker to execute unauthorized malicious script code via the "err" parameter of the error process HTTP requests. **CVE ID : CVE-2019-5588**	https://fortiguard.com/advisory/FG-IR-19-034	O-FOR-FORT-210619/492
Fujitsu					
arrows_nx_f005-f_firmware					
N/A	06-06-2019	1.9	Xiaomi Mi 5s Plus devices allow attackers to trigger touchscreen anomalies via a radio signal between 198 kHz and 203 kHz, as demonstrated by a transmitter and antenna hidden just beneath the surface of a coffee-shop table, aka Ghost Touch. **CVE ID : CVE-2019-12762**	N/A	O-FUJ-ARRO-210619/493
Google					
nexus_7_firmware					
N/A	06-06-2019	1.9	Xiaomi Mi 5s Plus devices allow attackers to trigger touchscreen	N/A	O-GOO-NEXU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			anomalies via a radio signal between 198 kHz and 203 kHz, as demonstrated by a transmitter and antenna hidden just beneath the surface of a coffee-shop table, aka Ghost Touch. **CVE ID : CVE-2019-12762**		210619/494
nexus_9_firmware					
N/A	06-06-2019	1.9	Xiaomi Mi 5s Plus devices allow attackers to trigger touchscreen anomalies via a radio signal between 198 kHz and 203 kHz, as demonstrated by a transmitter and antenna hidden just beneath the surface of a coffee-shop table, aka Ghost Touch. **CVE ID : CVE-2019-12762**	N/A	O-GOO-NEXU-210619/495
android					
N/A	07-06-2019	4.6	In isPackageDeviceAdminOnAnyUser of PackageManagerService.java, there is a possible permissions bypass due to a missing permissions check. This could lead to local escalation of privilege, with no additional permissions required. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-128599183 **CVE ID : CVE-2019-2090**	https://source.android.com/security/bulletin/2019-06-01	O-GOO-ANDR-210619/496
N/A	07-06-2019	7.2	In GetPermittedAccessibilityServicesForUser of DevicePolicyManagerService.java, there is a possible permissions	https://source.android.com/security/bulletin/2019-	O-GOO-ANDR-210619/497

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
			bypass due to a missing permission check. This could lead to local escalation of privilege, with no additional permissions required. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1. Android ID: A-128599660. **CVE ID : CVE-2019-2091**	06-01	
N/A	07-06-2019	7.2	In isSeparateProfileChallengeAllowed of DevicePolicyManagerService.java, there is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege, with no additional permissions required. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-128599668. **CVE ID : CVE-2019-2092**	https://source.android.com/security/bulletin/2019-06-01	O-GOO-ANDR-210619/498
Out-of-bounds Write	07-06-2019	9.3	In huff_dec_1D of nlc_dec.cpp, 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. Product: Android. Versions: Android-9. Android ID: A-119292397. **CVE ID : CVE-2019-2093**	https://source.android.com/security/bulletin/2019-06-01	O-GOO-ANDR-210619/499

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 Write	07-06-2019	9.3	In parseMPEGCCData of NuPlayerCCDecoder.cpp, there is a possible out of bounds write due to missing bounds checks. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-129068792. **CVE ID : CVE-2019-2094**	https://source.android.com/security/bulletin/2019-06-01	O-GOO-ANDR-210619/500
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	07-06-2019	7.6	In callGenIDChangeListeners and related functions of SkPixelRef.cpp, there is a possible use after free due to a race condition. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-124232283. **CVE ID : CVE-2019-2095**	https://source.android.com/security/bulletin/2019-06-01	O-GOO-ANDR-210619/501
Double Free	07-06-2019	7.2	In EffectRelease of EffectBundle.cpp, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege in the audio server with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-	https://source.android.com/security/bulletin/2019-06-01	O-GOO-ANDR-210619/502

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
			123237974. **CVE ID : CVE-2019-2096**		
Incorrect Type Conversion or Cast	07-06-2019	10	In HAliasAnalyzer.Query of hydrogen-alias-analysis.h, there is possible memory corruption due to type confusion. This could lead to remote code execution from a malicious proxy configuration, with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-117606285. **CVE ID : CVE-2019-2097**	https://source.android.com/security/bulletin/2019-06-01	O-GOO-ANDR-210619/503
N/A	07-06-2019	7.2	In areNotificationsEnabledForPackage of NotificationManagerService.java, there is a possible permissions bypass due to a missing permissions check. This could lead to local escalation of privilege, with no additional privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-128599467. **CVE ID : CVE-2019-2098**	https://source.android.com/security/bulletin/2019-06-01	O-GOO-ANDR-210619/504
Out-of-bounds Write	07-06-2019	9.3	In nfa_rw_store_ndef_rx_buf of nfa_rw_act.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of	https://source.android.com/security/bulletin/2019-	O-GOO-ANDR-210619/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-123583388. **CVE ID : CVE-2019-2099**	06-01	
Out-of-bounds Read	07-06-2019	4.9	In uvc_parse_standard_control of uvc_driver.c, there is a possible out-of-bound read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-111760968. **CVE ID : CVE-2019-2101**	https://source.android.com/security/bulletin/2019-06-01	O-GOO-ANDR-210619/506
N/A	07-06-2019	8.3	In the Bluetooth Low Energy (BLE) specification, there is a provided example Long Term Key (LTK). If a BLE device were to use this as a hardcoded LTK, it is theoretically possible for a proximate attacker to remotely inject keystrokes on a paired Android host due to improperly used crypto. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-128843052. **CVE ID : CVE-2019-2102**	https://source.android.com/security/bulletin/2019-06-01	O-GOO-ANDR-210619/507
HP					

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
integrated_lights-out_4_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-06-2019	7.6	A remote cross site scripting vulnerability was identified in HPE Integrated Lights-Out 4 (iLO 4) earlier than v2.61b for Gen9 servers and Integrated Lights-Out 5 (iLO 5) for Gen10 Servers earlier than version v1.39. **CVE ID : CVE-2019-11982**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03917en_us	O-HP-INTE-210619/508
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-06-2019	8.3	A remote buffer overflow vulnerability was identified in HPE Integrated Lights-Out 4 (iLO 4) earlier than v2.61b for Gen9 servers and Integrated Lights-Out 5 (iLO 5) for Gen10 Servers earlier than version v1.39. **CVE ID : CVE-2019-11983**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03917en_us	O-HP-INTE-210619/509
integrated_lights-out_5_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-06-2019	7.6	A remote cross site scripting vulnerability was identified in HPE Integrated Lights-Out 4 (iLO 4) earlier than v2.61b for Gen9 servers and Integrated Lights-Out 5 (iLO 5) for Gen10 Servers earlier than version v1.39. **CVE ID : CVE-2019-11982**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03917en_us	O-HP-INTE-210619/510
Improper Restriction of Operations within the	05-06-2019	8.3	A remote buffer overflow vulnerability was identified in HPE Integrated Lights-Out 4 (iLO 4) earlier than v2.61b for Gen9 servers and Integrated Lights-Out 5 (iLO 5) for Gen10 Servers	https://support.hpe.com/hpsc/doc/public/display?docLocale=en	O-HP-INTE-210619/511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			earlier than version v1.39. **CVE ID : CVE-2019-11983**	_US&docId=emr_na-hpesbhf03917en_us	
Huawei					
s5700_firmware					
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109) **CVE ID : CVE-2019-5285**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190522-01-switch-en	O-HUA-S570-210619/512
s600-e_firmware					
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109) **CVE ID : CVE-2019-5285**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190522-01-switch-en	O-HUA-S600-210619/513
s6300_firmware					
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the	https://www.huawei.com/en/psirt/securit	O-HUA-S630-210619/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device to exploit this vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109) **CVE ID : CVE-2019-5285**	y-advisories/huawei-sa-20190522-01-switch-en	
s6700_firmware					
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109) **CVE ID : CVE-2019-5285**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190522-01-switch-en	O-HUA-S670-210619/515
s7700_firmware					
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109) **CVE ID : CVE-2019-5285**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190522-01-switch-en	O-HUA-S770-210619/516
s7900_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109) **CVE ID : CVE-2019-5285**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190522-01-switch-en	O-HUA-S790-210619/517
s9300_firmware					
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109) **CVE ID : CVE-2019-5285**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190522-01-switch-en	O-HUA-S930-210619/518
s9300x_firmware					
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190522-01-switch-en	O-HUA-S930-210619/519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-03109) **CVE ID : CVE-2019-5285**		
s9700_firmware					
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109) **CVE ID : CVE-2019-5285**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190522-01-switch-en	O-HUA-S970-210619/520
ar1200-s_firmware					
Improper Verification of Cryptographic Signature	04-06-2019	4.6	There is a digital signature verification bypass vulnerability in AR1200, AR1200-S, AR150, AR160, AR200, AR2200, AR2200-S, AR3200, SRG1300, SRG2300 and SRG3300 Huawei routers. The vulnerability is due to the affected software improperly verifying digital signatures for the software image in the affected device. A local attacker with high privilege may exploit the vulnerability to bypass integrity checks for software images and install a malicious software image on the affected device. **CVE ID : CVE-2019-5300**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190320-01-ar-en	O-HUA-AR12-210619/521
ar1200_firmware					
Improper Verification of	04-06-2019	4.6	There is a digital signature verification bypass vulnerability in AR1200, AR1200-S, AR150,	https://www.huawei.com/en/p	O-HUA-AR12-210619/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Signature			AR160, AR200, AR2200, AR2200-S, AR3200, SRG1300, SRG2300 and SRG3300 Huawei routers. The vulnerability is due to the affected software improperly verifying digital signatures for the software image in the affected device. A local attacker with high privilege may exploit the vulnerability to bypass integrity checks for software images and install a malicious software image on the affected device. **CVE ID : CVE-2019-5300**	sirt/security-advisories/huawei-sa-20190320-01-ar-en	
ar150_firmware					
Improper Verification of Cryptographic Signature	04-06-2019	4.6	There is a digital signature verification bypass vulnerability in AR1200, AR1200-S, AR150, AR160, AR200, AR2200, AR2200-S, AR3200, SRG1300, SRG2300 and SRG3300 Huawei routers. The vulnerability is due to the affected software improperly verifying digital signatures for the software image in the affected device. A local attacker with high privilege may exploit the vulnerability to bypass integrity checks for software images and install a malicious software image on the affected device. **CVE ID : CVE-2019-5300**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190320-01-ar-en	O-HUA-AR15-210619/523
ar160_firmware					
Improper Verification of Cryptographic Signature	04-06-2019	4.6	There is a digital signature verification bypass vulnerability in AR1200, AR1200-S, AR150, AR160, AR200, AR2200, AR2200-S, AR3200, SRG1300, SRG2300 and SRG3300 Huawei routers.	https://www.huawei.com/en/psirt/security-advisories/	O-HUA-AR16-210619/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The vulnerability is due to the affected software improperly verifying digital signatures for the software image in the affected device. A local attacker with high privilege may exploit the vulnerability to bypass integrity checks for software images and install a malicious software image on the affected device. **CVE ID : CVE-2019-5300**	huawei-sa-20190320-01-ar-en	
ar200_firmware					
Improper Verification of Cryptographic Signature	04-06-2019	4.6	There is a digital signature verification bypass vulnerability in AR1200, AR1200-S, AR150, AR160, AR200, AR2200, AR2200-S, AR3200, SRG1300, SRG2300 and SRG3300 Huawei routers. The vulnerability is due to the affected software improperly verifying digital signatures for the software image in the affected device. A local attacker with high privilege may exploit the vulnerability to bypass integrity checks for software images and install a malicious software image on the affected device. **CVE ID : CVE-2019-5300**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190320-01-ar-en	O-HUA-AR20-210619/525
ar2200_firmware					
Improper Verification of Cryptographic Signature	04-06-2019	4.6	There is a digital signature verification bypass vulnerability in AR1200, AR1200-S, AR150, AR160, AR200, AR2200, AR2200-S, AR3200, SRG1300, SRG2300 and SRG3300 Huawei routers. The vulnerability is due to the affected software improperly verifying digital signatures for	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190320-01-ar-en	O-HUA-AR22-210619/526

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
			the software image in the affected device. A local attacker with high privilege may exploit the vulnerability to bypass integrity checks for software images and install a malicious software image on the affected device. **CVE ID : CVE-2019-5300**		
ar2200s_firmware					
Improper Verification of Cryptographic Signature	04-06-2019	4.6	There is a digital signature verification bypass vulnerability in AR1200, AR1200-S, AR150, AR160, AR200, AR2200, AR2200-S, AR3200, SRG1300, SRG2300 and SRG3300 Huawei routers. The vulnerability is due to the affected software improperly verifying digital signatures for the software image in the affected device. A local attacker with high privilege may exploit the vulnerability to bypass integrity checks for software images and install a malicious software image on the affected device. **CVE ID : CVE-2019-5300**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190320-01-ar-en	O-HUA-AR22-210619/527
ar3200_firmware					
Improper Verification of Cryptographic Signature	04-06-2019	4.6	There is a digital signature verification bypass vulnerability in AR1200, AR1200-S, AR150, AR160, AR200, AR2200, AR2200-S, AR3200, SRG1300, SRG2300 and SRG3300 Huawei routers. The vulnerability is due to the affected software improperly verifying digital signatures for the software image in the affected device. A local attacker with high privilege may exploit the	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190320-01-ar-en	O-HUA-AR32-210619/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass integrity checks for software images and install a malicious software image on the affected device. **CVE ID : CVE-2019-5300**		
srg1300_firmware					
Improper Verification of Cryptographic Signature	04-06-2019	4.6	There is a digital signature verification bypass vulnerability in AR1200, AR1200-S, AR150, AR160, AR200, AR2200, AR2200-S, AR3200, SRG1300, SRG2300 and SRG3300 Huawei routers. The vulnerability is due to the affected software improperly verifying digital signatures for the software image in the affected device. A local attacker with high privilege may exploit the vulnerability to bypass integrity checks for software images and install a malicious software image on the affected device. **CVE ID : CVE-2019-5300**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190320-01-ar-en	O-HUA-SRG1-210619/529
srg2300_firmware					
Improper Verification of Cryptographic Signature	04-06-2019	4.6	There is a digital signature verification bypass vulnerability in AR1200, AR1200-S, AR150, AR160, AR200, AR2200, AR2200-S, AR3200, SRG1300, SRG2300 and SRG3300 Huawei routers. The vulnerability is due to the affected software improperly verifying digital signatures for the software image in the affected device. A local attacker with high privilege may exploit the vulnerability to bypass integrity checks for software images and install a malicious software image	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190320-01-ar-en	O-HUA-SRG2-210619/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on the affected device. **CVE ID : CVE-2019-5300**		
srg3300_firmware					
Improper Verification of Cryptographic Signature	04-06-2019	4.6	There is a digital signature verification bypass vulnerability in AR1200, AR1200-S, AR150, AR160, AR200, AR2200, AR2200-S, AR3200, SRG1300, SRG2300 and SRG3300 Huawei routers. The vulnerability is due to the affected software improperly verifying digital signatures for the software image in the affected device. A local attacker with high privilege may exploit the vulnerability to bypass integrity checks for software images and install a malicious software image on the affected device. **CVE ID : CVE-2019-5300**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190320-01-ar-en	O-HUA-SRG3-210619/531
hg255s_firmware					
Improper Input Validation	10-06-2019	4.3	There is a Clickjacking vulnerability in Huawei HG255s product. An attacker may trick user to click a link and affect the integrity of a device by exploiting this vulnerability. **CVE ID : CVE-2019-5243**	N/A	O-HUA-HG25-210619/532
s12700_firmware					
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190522-01-switch-	O-HUA-S127-210619/533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109) **CVE ID : CVE-2019-5285**	en	
s1700_firmware					
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109) **CVE ID : CVE-2019-5285**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190522-01-switch-en	O-HUA-S170-210619/534
s2300_firmware					
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109) **CVE ID : CVE-2019-5285**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190522-01-switch-en	O-HUA-S230-210619/535
s2700_firmware					
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this	https://www.huawei.com/en/psirt/security-	O-HUA-S270-210619/536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109) **CVE ID : CVE-2019-5285**	advisories/huawei-sa-20190522-01-switch-en	
s5300_firmware					
Improper Input Validation	04-06-2019	7.8	Some Huawei S series switches have a DoS vulnerability. An unauthenticated remote attacker can send crafted packets to the affected device to exploit this vulnerability. Due to insufficient verification of the packets, successful exploitation may cause the device reboot and denial of service (DoS) condition. (Vulnerability ID: HWPSIRT-2019-03109) **CVE ID : CVE-2019-5285**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190522-01-switch-en	O-HUA-S530-210619/537
Kyocera					
command_center_rx					
N/A	06-06-2019	4	Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password. **CVE ID : CVE-2019-6452**	N/A	O-KYO-COMM-210619/538
Linksys					
wrt1900acs_firmware					
N/A	06-06-2019	7.2	An issue was discovered on Linksys WRT1900ACS 1.0.3.187766 devices. A lack of encryption in how the user login	N/A	O-LIN-WRT1-210619/539

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
			cookie (admin-auth) is stored on a victim's computer results in the admin password being discoverable by a local attacker, and usable to gain administrative access to the victim's router. The admin password is stored in base64 cleartext in an "admin-auth" cookie. An attacker sniffing the network at the time of login could acquire the router's admin password. Alternatively, gaining physical access to the victim's computer soon after an administrative login could result in compromise. **CVE ID : CVE-2019-7311**		
Linux					
linux_kernel					
NULL Pointer Dereference	03-06-2019	7.8	An issue was discovered in dlpar_parse_cc_property in arch/powerpc/platforms/pseries/dlpar.c in the Linux kernel through 5.1.6. There is an unchecked kstrdup of prop->name, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). **CVE ID : CVE-2019-12614**	N/A	O-LIN-LINU-210619/540
NULL Pointer Dereference	03-06-2019	7.8	An issue was discovered in get_vdev_port_node_info in arch/sparc/kernel/mdesc.c in the Linux kernel through 5.1.6. There is an unchecked kstrdup_const of node_info->vdev_port.name, which might allow an attacker to cause a denial of service (NULL pointer	N/A	O-LIN-LINU-210619/541

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
			dereference and system crash). **CVE ID : CVE-2019-12615**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2019	8.3	A flaw that allowed an attacker to corrupt memory and possibly escalate privileges was found in the mwifiex kernel module while connecting to a malicious wireless network. **CVE ID : CVE-2019-3846**	N/A	O-LIN-LINU-210619/542
Logitech					
r700_laser_presentation_remote_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	07-06-2019	8.3	Due to unencrypted and unauthenticated data communication, the wireless presenter Logitech R700 Laser Presentation Remote R-R0010 is prone to keystroke injection attacks. Thus, an attacker is able to send arbitrary keystrokes to a victim's computer system, e.g., to install malware when the target system is unattended. In this way, an attacker can remotely take control over the victim's computer that is operated with an affected receiver of this device. **CVE ID : CVE-2019-12506**	N/A	O-LOG-R700-210619/543
Marvell					
88ss1074_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090,	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/544

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
			88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**		
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/545
88ss1079_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/546
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088,	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/547

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
			& 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**		
88ss1080_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/548
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/549
88ss1084_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090,	https://www.marvell.com/documents/x9g4hrszt5ls3	O-MAR-88SS-210619/550

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
			88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	udbe1eo/	
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/551
88ss1085_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/552
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088,	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/553

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
			& 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**		
88ss1087_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/554
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/555
88ss1088_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090,	https://www.marvell.com/documents/x9g4hrszt5ls3	O-MAR-88SS-210619/556

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
			88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	udbe1eo/	
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/557
88ss1090_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/558
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088,	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/559

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
			& 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**		
88ss1092_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/560
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/561
88ss1093_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090,	https://www.marvell.com/documents/x9g4hrszt5ls3	O-MAR-88SS-210619/562

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
			88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	udbe1eo/	
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/563
88ss1095_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/564
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088,	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/565

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
			& 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**		
88ss1098_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/566
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/567
88ss1100_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090,	https://www.marvell.com/documents/x9g4hrszt5ls3	O-MAR-88SS-210619/568

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
			88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	udbe1eo/	
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/569
88ss9174_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/570
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088,	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			& 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**		
88ss9175_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/572
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/573
88ss9187_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090,	https://www.marvell.com/documents/x9g4hrszt5ls3	O-MAR-88SS-210619/574

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
			88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	udbe1eo/	
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/575
88ss9188_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/576
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088,	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/577

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
			& 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**		
88ss9189_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/578
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/579
88ss9190_firmware					
N/A	04-06-2019	4.9	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090,	https://www.marvell.com/documents/x9g4hrszt5ls3	O-MAR-88SS-210619/580

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
			88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices allow reprogramming flash memory to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10636**	udbe1eo/	
N/A	05-06-2019	2.1	Marvell SSD Controller (88SS1074, 88SS1079, 88SS1080, 88SS1093, 88SS1092, 88SS1095, 88SS9174, 88SS9175, 88SS9187, 88SS9188, 88SS9189, 88SS9190, 88SS1085, 88SS1087, 88SS1090, 88SS1100, 88SS1084, 88SS1088, & 88SS1098) devices are vulnerable in manipulating a combination of IO pins to bypass the secure boot protection mechanism. **CVE ID : CVE-2019-10637**	https://www.marvell.com/documents/x9g4hrszt5ls3udbe1eo/	O-MAR-88SS-210619/581
Microsoft					
azure_devops_server_2019					
Cross-Site Request Forgery (CSRF)	12-06-2019	4.3	A spoofing vulnerability exists in Azure DevOps Server when it improperly handles requests to authorize applications, resulting in a cross-site request forgery, aka 'Azure DevOps Server Spoofing Vulnerability'. **CVE ID : CVE-2019-0996**	N/A	O-MIC-AZUR-210619/582
windows_10					
Improper Restriction of Operations within the Bounds of a	12-06-2019	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-2019-0905,	N/A	O-MIC-WIND-210619/583

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			CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0904**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0905**	N/A	O-MIC-WIND-210619/584
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0906**	N/A	O-MIC-WIND-210619/585
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974.	N/A	O-MIC-WIND-210619/586

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-2019-0907		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0908**	N/A	O-MIC-WIND-210619/587
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0974. **CVE ID : CVE-2019-0909**	N/A	O-MIC-WIND-210619/588
Improper Input Validation	12-06-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0709, CVE-2019-0722. **CVE ID : CVE-2019-0620**	N/A	O-MIC-WIND-210619/589
Improper Input Validatio	12-06-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host	N/A	O-MIC-WIND-210619/590

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
n			server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0620, CVE-2019-0722. **CVE ID : CVE-2019-0709**		
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0711, CVE-2019-0713. **CVE ID : CVE-2019-0710**	N/A	O-MIC-WIND-210619/591
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0713. **CVE ID : CVE-2019-0711**	N/A	O-MIC-WIND-210619/592
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0711. **CVE ID : CVE-2019-0713**	N/A	O-MIC-WIND-210619/593

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	12-06-2019	9	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0620, CVE-2019-0709. **CVE ID : CVE-2019-0722**	N/A	O-MIC-WIND-210619/594
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in the way that ActiveX Data Objects (ADO) handle objects in memory, aka 'ActiveX Data Objects (ADO) Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0888**	N/A	O-MIC-WIND-210619/595
N/A	12-06-2019	5	A denial of service exists in Microsoft IIS Server when the optional request filtering feature improperly handles requests, aka 'Microsoft IIS Server Denial of Service Vulnerability'. **CVE ID : CVE-2019-0941**	N/A	O-MIC-WIND-210619/596
N/A	12-06-2019	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'.	N/A	O-MIC-WIND-210619/597

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-2019-0943		
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists in the Windows Event Viewer (eventvwr.msc) when it improperly parses XML input containing a reference to an external entity, aka 'Windows Event Viewer Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0948**	N/A	O-MIC-WIND-210619/598
N/A	12-06-2019	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'. This CVE ID is unique from CVE-2019-0984. **CVE ID : CVE-2019-0959**	N/A	O-MIC-WIND-210619/599
N/A	12-06-2019	6.8	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2019-0972**	N/A	O-MIC-WIND-210619/600
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated	N/A	O-MIC-WIND-210619/601

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
			attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0973**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909. **CVE ID : CVE-2019-0974**	N/A	O-MIC-WIND-210619/602
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0998. **CVE ID : CVE-2019-0983**	N/A	O-MIC-WIND-210619/603
N/A	12-06-2019	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'. This CVE ID is unique from CVE-2019-0959. **CVE ID : CVE-2019-0984**	N/A	O-MIC-WIND-210619/604
N/A	12-06-2019	3.6	An elevation of privilege 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
			Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0986**		210619/605
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1012**	N/A	O-MIC-WIND-210619/606
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0983. **CVE ID : CVE-2019-0998**	N/A	O-MIC-WIND-210619/607
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1021, CVE-2019-1022, CVE-2019-1026, CVE-2019-1027, CVE-2019-1028. **CVE ID : CVE-2019-1007**	N/A	O-MIC-WIND-210619/608

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	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1010**	N/A	O-MIC-WIND-210619/609
N/A	12-06-2019	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-2019-0960, CVE-2019-1017. **CVE ID : CVE-2019-1014**	N/A	O-MIC-WIND-210619/610
N/A	12-06-2019	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-2019-0960, CVE-2019-1014. **CVE ID : CVE-2019-1017**	N/A	O-MIC-WIND-210619/611
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1018**	N/A	O-MIC-WIND-210619/612

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
N/A	12-06-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1019**	N/A	O-MIC-WIND-210619/613
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1022, CVE-2019-1026, CVE-2019-1027, CVE-2019-1028. **CVE ID : CVE-2019-1021**	N/A	O-MIC-WIND-210619/614
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1026, CVE-2019-1027, CVE-2019-1028. **CVE ID : CVE-2019-1022**	N/A	O-MIC-WIND-210619/615
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	7.8	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-1025**	N/A	O-MIC-WIND-210619/616

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
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1027, CVE-2019-1028. **CVE ID : CVE-2019-1026**	N/A	O-MIC-WIND-210619/617
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1026, CVE-2019-1028. **CVE ID : CVE-2019-1027**	N/A	O-MIC-WIND-210619/618
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1026, CVE-2019-1027. **CVE ID : CVE-2019-1028**	N/A	O-MIC-WIND-210619/619
Information Exposure	12-06-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1039**	N/A	O-MIC-WIND-210619/620
N/A	12-06-2019	4.3	A tampering vulnerability exists in Microsoft Windows when a	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
			man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'. **CVE ID : CVE-2019-1040**		210619/621
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1065. **CVE ID : CVE-2019-1041**	N/A	O-MIC-WIND-210619/622
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	8.5	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1043**	N/A	O-MIC-WIND-210619/623
N/A	12-06-2019	7.2	A security feature bypass vulnerability exists when Windows Secure Kernel Mode fails to properly handle objects in memory.To exploit the vulnerability, a locally-authenticated attacker could attempt to run a specially crafted application on a targeted system, aka 'Windows Secure Kernel Mode Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1044**	N/A	O-MIC-WIND-210619/624
N/A	12-06-2019	7.2	An elevation of privilege	N/A	O-MIC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists in the way that the Windows Network File System (NFS) handles objects in memory, aka 'Windows Network File System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1045**		WIND-210619/625
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1046**	N/A	O-MIC-WIND-210619/626
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049. **CVE ID : CVE-2019-1050**	N/A	O-MIC-WIND-210619/627
N/A	12-06-2019	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
			Windows Shell fails to validate folder shortcuts, aka 'Windows Shell Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1053**		210619/628
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1064**	N/A	O-MIC-WIND-210619/629
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1041. **CVE ID : CVE-2019-1065**	N/A	O-MIC-WIND-210619/630
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the way the Task Scheduler Service validates certain file operations, aka 'Task Scheduler Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1069**	N/A	O-MIC-WIND-210619/631
windows_7					
Improper Restriction of Operations within the Bounds of a	12-06-2019	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-2019-0905,	N/A	O-MIC-WIND-210619/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0904**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0905**	N/A	O-MIC-WIND-210619/633
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0906**	N/A	O-MIC-WIND-210619/634
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974.	N/A	O-MIC-WIND-210619/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0907		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0908**	N/A	O-MIC-WIND-210619/636
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0974. **CVE ID : CVE-2019-0909**	N/A	O-MIC-WIND-210619/637
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0711. **CVE ID : CVE-2019-0713**	N/A	O-MIC-WIND-210619/638
Improper Input Validation	12-06-2019	9	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate	N/A	O-MIC-WIND-210619/639

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 from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0620, CVE-2019-0709. **CVE ID : CVE-2019-0722**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in the way that ActiveX Data Objects (ADO) handle objects in memory, aka 'ActiveX Data Objects (ADO) Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0888**	N/A	O-MIC-WIND-210619/640
N/A	12-06-2019	5	A denial of service exists in Microsoft IIS Server when the optional request filtering feature improperly handles requests, aka 'Microsoft IIS Server Denial of Service Vulnerability'. **CVE ID : CVE-2019-0941**	N/A	O-MIC-WIND-210619/641
N/A	12-06-2019	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'. **CVE ID : CVE-2019-0943**	N/A	O-MIC-WIND-210619/642
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists in the Windows Event Viewer	N/A	O-MIC-WIND-210619/643

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
			(eventvwr.msc) when it improperly parses XML input containing a reference to an external entity, aka 'Windows Event Viewer Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0948**		
N/A	12-06-2019	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-2019-1014, CVE-2019-1017. **CVE ID : CVE-2019-0960**	N/A	O-MIC-WIND-210619/644
Information Exposure	12-06-2019	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-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-0968**	N/A	O-MIC-WIND-210619/645
N/A	12-06-2019	6.8	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service	N/A	O-MIC-WIND-210619/646

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
			Denial of Service Vulnerability'. **CVE ID : CVE-2019-0972**		
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0973**	N/A	O-MIC-WIND-210619/647
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909. **CVE ID : CVE-2019-0974**	N/A	O-MIC-WIND-210619/648
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048,	N/A	O-MIC-WIND-210619/649

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-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-0977**		
N/A	12-06-2019	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'. This CVE ID is unique from CVE-2019-0959. **CVE ID : CVE-2019-0984**	N/A	O-MIC-WIND-210619/650
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	6.8	A remote code execution vulnerability exists when the Microsoft Speech API (SAPI) improperly handles text-to-speech (TTS) input, aka 'Microsoft Speech API Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0985**	N/A	O-MIC-WIND-210619/651
N/A	12-06-2019	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0986**	N/A	O-MIC-WIND-210619/652
Information Exposure	12-06-2019	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-2019-0968,	N/A	O-MIC-WIND-210619/653

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
			CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1011**		
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1012**	N/A	O-MIC-WIND-210619/654
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1013**	N/A	O-MIC-WIND-210619/655
Information	12-06-2019	4.3	An information disclosure vulnerability exists when the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0968, CVE-2019-0977, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1009**		210619/656
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1010**	N/A	O-MIC-WIND-210619/657
N/A	12-06-2019	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-2019-0960, CVE-2019-1017. **CVE ID : CVE-2019-1014**	N/A	O-MIC-WIND-210619/658
Information	12-06-2019	4.3	An information disclosure vulnerability exists when the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1015**		210619/659
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1016**	N/A	O-MIC-WIND-210619/660
N/A	12-06-2019	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-2019-0960, CVE-2019-1014. **CVE ID : CVE-2019-1017**	N/A	O-MIC-WIND-210619/661
N/A	12-06-2019	6.5	A security feature bypass vulnerability exists where a	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1019**		210619/662
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	7.8	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-1025**	N/A	O-MIC-WIND-210619/663
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1026, CVE-2019-1027. **CVE ID : CVE-2019-1028**	N/A	O-MIC-WIND-210619/664
Information Exposure	12-06-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1039**	N/A	O-MIC-WIND-210619/665
N/A	12-06-2019	4.3	A tampering vulnerability exists	N/A	O-MIC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'. **CVE ID : CVE-2019-1040**		WIND-210619/666
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	8.5	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1043**	N/A	O-MIC-WIND-210619/667
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the way that the Windows Network File System (NFS) handles objects in memory, aka 'Windows Network File System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1045**	N/A	O-MIC-WIND-210619/668
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050.	N/A	O-MIC-WIND-210619/669

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-2019-1046		
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1047**	N/A	O-MIC-WIND-210619/670
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1048**	N/A	O-MIC-WIND-210619/671
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009,	N/A	O-MIC-WIND-210619/672

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-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1050. **CVE ID : CVE-2019-1049**		
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows Shell fails to validate folder shortcuts, aka 'Windows Shell Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1053**	N/A	O-MIC-WIND-210619/673
windows_8.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0904**	N/A	O-MIC-WIND-210619/674
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0905**	N/A	O-MIC-WIND-210619/675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0906**	N/A	O-MIC-WIND-210619/676
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0907**	N/A	O-MIC-WIND-210619/677
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0908**	N/A	O-MIC-WIND-210619/678
Improper Restriction of	12-06-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine	N/A	O-MIC-WIND-210619/679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0974. **CVE ID : CVE-2019-0909**		
Improper Input Validation	12-06-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0709, CVE-2019-0722. **CVE ID : CVE-2019-0620**	N/A	O-MIC-WIND-210619/680
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0711, CVE-2019-0713. **CVE ID : CVE-2019-0710**	N/A	O-MIC-WIND-210619/681
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0713.	N/A	O-MIC-WIND-210619/682

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-2019-0711		
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0711. **CVE ID : CVE-2019-0713**	N/A	O-MIC-WIND-210619/683
Improper Input Validation	12-06-2019	9	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0620, CVE-2019-0709. **CVE ID : CVE-2019-0722**	N/A	O-MIC-WIND-210619/684
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in the way that ActiveX Data Objects (ADO) handle objects in memory, aka 'ActiveX Data Objects (ADO) Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0888**	N/A	O-MIC-WIND-210619/685
N/A	12-06-2019	5	A denial of service exists in Microsoft IIS Server when the optional request filtering feature improperly handles requests, aka 'Microsoft IIS Server Denial of Service Vulnerability'. **CVE ID : CVE-2019-0941**	N/A	O-MIC-WIND-210619/686

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
N/A	12-06-2019	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'. **CVE ID : CVE-2019-0943**	N/A	O-MIC-WIND-210619/687
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists in the Windows Event Viewer (eventvwr.msc) when it improperly parses XML input containing a reference to an external entity, aka 'Windows Event Viewer Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0948**	N/A	O-MIC-WIND-210619/688
N/A	12-06-2019	6.8	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2019-0972**	N/A	O-MIC-WIND-210619/689
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated	N/A	O-MIC-WIND-210619/690

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
			attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0973**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909. **CVE ID : CVE-2019-0974**	N/A	O-MIC-WIND-210619/691
N/A	12-06-2019	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'. This CVE ID is unique from CVE-2019-0959. **CVE ID : CVE-2019-0984**	N/A	O-MIC-WIND-210619/692
N/A	12-06-2019	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0986**	N/A	O-MIC-WIND-210619/693
Information	12-06-2019	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
Exposure			improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1012**		210619/694
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1010**	N/A	O-MIC-WIND-210619/695
N/A	12-06-2019	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-2019-0960, CVE-2019-1017. **CVE ID : CVE-2019-1014**	N/A	O-MIC-WIND-210619/696
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component	N/A	O-MIC-WIND-210619/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0960, CVE-2019-1014. **CVE ID : CVE-2019-1017**		
N/A	12-06-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1019**	N/A	O-MIC-WIND-210619/698
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	7.8	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-1025**	N/A	O-MIC-WIND-210619/699
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1026, CVE-2019-1027. **CVE ID : CVE-2019-1028**	N/A	O-MIC-WIND-210619/700
Information Exposure	12-06-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly	N/A	O-MIC-WIND-210619/701

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
			initializes objects in memory.To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1039**		
N/A	12-06-2019	4.3	A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'. **CVE ID : CVE-2019-1040**	N/A	O-MIC-WIND-210619/702
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	8.5	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1043**	N/A	O-MIC-WIND-210619/703
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the way that the Windows Network File System (NFS) handles objects in memory, aka 'Windows Network File System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1045**	N/A	O-MIC-WIND-210619/704
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure	N/A	O-MIC-WIND-210619/705

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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1046**		
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049. **CVE ID : CVE-2019-1050**	N/A	O-MIC-WIND-210619/706
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows Shell fails to validate folder shortcuts, aka 'Windows Shell Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1053**	N/A	O-MIC-WIND-210619/707
windows_rt_8.1					
Improper Restriction of Operations within the Bounds	12-06-2019	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-210619/708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Memory Buffer			unique from CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0904**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0905**	N/A	O-MIC-WIND-210619/709
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0906**	N/A	O-MIC-WIND-210619/710
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0908, CVE-2019-0909,	N/A	O-MIC-WIND-210619/711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-0974. **CVE ID : CVE-2019-0907**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0908**	N/A	O-MIC-WIND-210619/712
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0974. **CVE ID : CVE-2019-0909**	N/A	O-MIC-WIND-210619/713
Improper Input Validation	12-06-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0709, CVE-2019-0722. **CVE ID : CVE-2019-0620**	N/A	O-MIC-WIND-210619/714
Improper Input	12-06-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on	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			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'. This CVE ID is unique from CVE-2019-0711, CVE-2019-0713. **CVE ID : CVE-2019-0710**		210619/715
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0713. **CVE ID : CVE-2019-0711**	N/A	O-MIC-WIND-210619/716
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0711. **CVE ID : CVE-2019-0713**	N/A	O-MIC-WIND-210619/717
Improper Input Validation	12-06-2019	9	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0620, CVE-2019-0709. **CVE ID : CVE-2019-0722**	N/A	O-MIC-WIND-210619/718

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	12-06-2019	9.3	A remote code execution vulnerability exists in the way that ActiveX Data Objects (ADO) handle objects in memory, aka 'ActiveX Data Objects (ADO) Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0888**	N/A	O-MIC-WIND-210619/719
N/A	12-06-2019	5	A denial of service exists in Microsoft IIS Server when the optional request filtering feature improperly handles requests, aka 'Microsoft IIS Server Denial of Service Vulnerability'. **CVE ID : CVE-2019-0941**	N/A	O-MIC-WIND-210619/720
N/A	12-06-2019	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'. **CVE ID : CVE-2019-0943**	N/A	O-MIC-WIND-210619/721
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists in the Windows Event Viewer (eventvwr.msc) when it improperly parses XML input containing a reference to an external entity, aka 'Windows Event Viewer Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0948**	N/A	O-MIC-WIND-210619/722

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
N/A	12-06-2019	6.8	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2019-0972**	N/A	O-MIC-WIND-210619/723
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0973**	N/A	O-MIC-WIND-210619/724
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909. **CVE ID : CVE-2019-0974**	N/A	O-MIC-WIND-210619/725
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka	N/A	O-MIC-WIND-210619/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0959. **CVE ID : CVE-2019-0984**		
N/A	12-06-2019	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0986**	N/A	O-MIC-WIND-210619/727
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1012**	N/A	O-MIC-WIND-210619/728
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1011, CVE-2019-1012,	N/A	O-MIC-WIND-210619/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1010**		
N/A	12-06-2019	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-2019-0960, CVE-2019-1017. **CVE ID : CVE-2019-1014**	N/A	O-MIC-WIND-210619/730
N/A	12-06-2019	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-2019-0960, CVE-2019-1014. **CVE ID : CVE-2019-1017**	N/A	O-MIC-WIND-210619/731
N/A	12-06-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1019**	N/A	O-MIC-WIND-210619/732
Improper Restriction of Operations within	12-06-2019	7.8	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service	N/A	O-MIC-WIND-210619/733

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
the Bounds of a Memory Buffer			Vulnerability'. **CVE ID : CVE-2019-1025**		
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1026, CVE-2019-1027. **CVE ID : CVE-2019-1028**	N/A	O-MIC-WIND-210619/734
Information Exposure	12-06-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1039**	N/A	O-MIC-WIND-210619/735
N/A	12-06-2019	4.3	A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'. **CVE ID : CVE-2019-1040**	N/A	O-MIC-WIND-210619/736
Improper Restriction of Operations within the Bounds	12-06-2019	8.5	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-210619/737

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 a Memory Buffer			**CVE ID : CVE-2019-1043**		
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the way that the Windows Network File System (NFS) handles objects in memory, aka 'Windows Network File System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1045**	N/A	O-MIC-WIND-210619/738
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1046**	N/A	O-MIC-WIND-210619/739
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047,	N/A	O-MIC-WIND-210619/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-1048, CVE-2019-1049. **CVE ID : CVE-2019-1050**		
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows Shell fails to validate folder shortcuts, aka 'Windows Shell Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1053**	N/A	O-MIC-WIND-210619/741
windows_server_2008					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0904**	N/A	O-MIC-WIND-210619/742
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0905**	N/A	O-MIC-WIND-210619/743
Improper Restriction of Operatio	12-06-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in	N/A	O-MIC-WIND-210619/744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ns within the Bounds of a Memory Buffer			memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0904, CVE-2019-0905, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0906**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0907**	N/A	O-MIC-WIND-210619/745
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0908**	N/A	O-MIC-WIND-210619/746
Improper Restriction of Operations within the Bounds	12-06-2019	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-210619/747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Memory Buffer			unique from CVE-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0974. **CVE ID : CVE-2019-0909**		
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0711. **CVE ID : CVE-2019-0713**	N/A	O-MIC-WIND-210619/748
Improper Input Validation	12-06-2019	9	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0620, CVE-2019-0709. **CVE ID : CVE-2019-0722**	N/A	O-MIC-WIND-210619/749
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in the way that ActiveX Data Objects (ADO) handle objects in memory, aka 'ActiveX Data Objects (ADO) Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0888**	N/A	O-MIC-WIND-210619/750
N/A	12-06-2019	5	A denial of service exists in Microsoft IIS Server when the optional request filtering feature	N/A	O-MIC-WIND-210619/751

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 handles requests, aka 'Microsoft IIS Server Denial of Service Vulnerability'. **CVE ID : CVE-2019-0941**		
N/A	12-06-2019	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'. **CVE ID : CVE-2019-0943**	N/A	O-MIC-WIND-210619/752
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists in the Windows Event Viewer (eventvwr.msc) when it improperly parses XML input containing a reference to an external entity, aka 'Windows Event Viewer Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0948**	N/A	O-MIC-WIND-210619/753
N/A	12-06-2019	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-2019-1014, CVE-2019-1017. **CVE ID : CVE-2019-0960**	N/A	O-MIC-WIND-210619/754
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents	N/A	O-MIC-WIND-210619/755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-0968**		
N/A	12-06-2019	6.8	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2019-0972**	N/A	O-MIC-WIND-210619/756
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0973**	N/A	O-MIC-WIND-210619/757
Improper Restriction of Operations within the	12-06-2019	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-210619/758

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			Vulnerability'. This CVE ID is unique from CVE-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909. **CVE ID : CVE-2019-0974**		
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-0977**	N/A	O-MIC-WIND-210619/759
N/A	12-06-2019	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'. This CVE ID is unique from CVE-2019-0959. **CVE ID : CVE-2019-0984**	N/A	O-MIC-WIND-210619/760
Improper Restriction of Operations within the Bounds	12-06-2019	6.8	A remote code execution vulnerability exists when the Microsoft Speech API (SAPI) improperly handles text-to-speech (TTS) input, aka 'Microsoft Speech API Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-210619/761

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 a Memory Buffer			**CVE ID : CVE-2019-0985**		
N/A	12-06-2019	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0986**	N/A	O-MIC-WIND-210619/762
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1011**	N/A	O-MIC-WIND-210619/763
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048,	N/A	O-MIC-WIND-210619/764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1012**		
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1013**	N/A	O-MIC-WIND-210619/765
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1009**	N/A	O-MIC-WIND-210619/766
Information Exposure	12-06-2019	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	N/A	O-MIC-WIND-210619/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1010**		
N/A	12-06-2019	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-2019-0960, CVE-2019-1017. **CVE ID : CVE-2019-1014**	N/A	O-MIC-WIND-210619/768
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1015**	N/A	O-MIC-WIND-210619/769
Information Exposure	12-06-2019	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	N/A	O-MIC-WIND-210619/770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1016**		
N/A	12-06-2019	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-2019-0960, CVE-2019-1014. **CVE ID : CVE-2019-1017**	N/A	O-MIC-WIND-210619/771
N/A	12-06-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1019**	N/A	O-MIC-WIND-210619/772
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	7.8	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-1025**	N/A	O-MIC-WIND-210619/773
N/A	12-06-2019	4.6	An elevation of privilege exists in	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
			Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1026, CVE-2019-1027. **CVE ID : CVE-2019-1028**		WIND-210619/774
Information Exposure	12-06-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1039**	N/A	O-MIC-WIND-210619/775
N/A	12-06-2019	4.3	A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'. **CVE ID : CVE-2019-1040**	N/A	O-MIC-WIND-210619/776
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	8.5	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1043**	N/A	O-MIC-WIND-210619/777
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the way that the Windows Network File	N/A	O-MIC-WIND-210619/778

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
			System (NFS) handles objects in memory, aka 'Windows Network File System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1045**		
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1046**	N/A	O-MIC-WIND-210619/779
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1047**	N/A	O-MIC-WIND-210619/780
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents	N/A	O-MIC-WIND-210619/781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1048**		
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1050. **CVE ID : CVE-2019-1049**	N/A	O-MIC-WIND-210619/782
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows Shell fails to validate folder shortcuts, aka 'Windows Shell Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1053**	N/A	O-MIC-WIND-210619/783
windows_server_2012					
Improper Restriction of Operations within	12-06-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine	N/A	O-MIC-WIND-210619/784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
the Bounds of a Memory Buffer			Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0904**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0905**	N/A	O-MIC-WIND-210619/785
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0906**	N/A	O-MIC-WIND-210619/786
Improper Restriction of Operations within the Bounds of a	12-06-2019	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-2019-0904,	N/A	O-MIC-WIND-210619/787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			CVE-2019-0905, CVE-2019-0906, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0907**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0908**	N/A	O-MIC-WIND-210619/788
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0974. **CVE ID : CVE-2019-0909**	N/A	O-MIC-WIND-210619/789
Improper Input Validation	12-06-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0709, CVE-2019-0722. **CVE ID : CVE-2019-0620**	N/A	O-MIC-WIND-210619/790

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	12-06-2019	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'. This CVE ID is unique from CVE-2019-0711, CVE-2019-0713. **CVE ID : CVE-2019-0710**	N/A	O-MIC-WIND-210619/791
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0713. **CVE ID : CVE-2019-0711**	N/A	O-MIC-WIND-210619/792
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0711. **CVE ID : CVE-2019-0713**	N/A	O-MIC-WIND-210619/793
Improper Input Validation	12-06-2019	9	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-	N/A	O-MIC-WIND-210619/794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0620, CVE-2019-0709. **CVE ID : CVE-2019-0722**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in the way that ActiveX Data Objects (ADO) handle objects in memory, aka 'ActiveX Data Objects (ADO) Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0888**	N/A	O-MIC-WIND-210619/795
N/A	12-06-2019	5	A denial of service exists in Microsoft IIS Server when the optional request filtering feature improperly handles requests, aka 'Microsoft IIS Server Denial of Service Vulnerability'. **CVE ID : CVE-2019-0941**	N/A	O-MIC-WIND-210619/796
N/A	12-06-2019	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'. **CVE ID : CVE-2019-0943**	N/A	O-MIC-WIND-210619/797
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists in the Windows Event Viewer (eventvwr.msc) when it improperly parses XML input containing a reference to an external entity, aka 'Windows Event Viewer Information	N/A	O-MIC-WIND-210619/798

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-2019-0948**		
N/A	12-06-2019	6.8	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2019-0972**	N/A	O-MIC-WIND-210619/799
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0973**	N/A	O-MIC-WIND-210619/800
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909. **CVE ID : CVE-2019-0974**	N/A	O-MIC-WIND-210619/801
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows Common Log File	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
			System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0959. **CVE ID : CVE-2019-0984**		210619/802
N/A	12-06-2019	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0986**	N/A	O-MIC-WIND-210619/803
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1012**	N/A	O-MIC-WIND-210619/804
Information Exposure	12-06-2019	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-2019-0968,	N/A	O-MIC-WIND-210619/805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-0977, CVE-2019-1009, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1010**		
N/A	12-06-2019	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-2019-0960, CVE-2019-1017. **CVE ID : CVE-2019-1014**	N/A	O-MIC-WIND-210619/806
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1015**	N/A	O-MIC-WIND-210619/807
N/A	12-06-2019	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-2019-0960, CVE-2019-1014.	N/A	O-MIC-WIND-210619/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1017		
N/A	12-06-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1019**	N/A	O-MIC-WIND-210619/809
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	7.8	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-1025**	N/A	O-MIC-WIND-210619/810
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1026, CVE-2019-1027. **CVE ID : CVE-2019-1028**	N/A	O-MIC-WIND-210619/811
Information Exposure	12-06-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information	N/A	O-MIC-WIND-210619/812

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-2019-1039**		
N/A	12-06-2019	4.3	A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'. **CVE ID : CVE-2019-1040**	N/A	O-MIC-WIND-210619/813
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	8.5	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1043**	N/A	O-MIC-WIND-210619/814
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the way that the Windows Network File System (NFS) handles objects in memory, aka 'Windows Network File System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1045**	N/A	O-MIC-WIND-210619/815
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013,	N/A	O-MIC-WIND-210619/816

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-2019-1015, CVE-2019-1016, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1046**		
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049. **CVE ID : CVE-2019-1050**	N/A	O-MIC-WIND-210619/817
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows Shell fails to validate folder shortcuts, aka 'Windows Shell Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1053**	N/A	O-MIC-WIND-210619/818
windows_server_2016					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974.	N/A	O-MIC-WIND-210619/819

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-2019-0904		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0905**	N/A	O-MIC-WIND-210619/820
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0906**	N/A	O-MIC-WIND-210619/821
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0907**	N/A	O-MIC-WIND-210619/822
Improper Restrictio	12-06-2019	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
n 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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0908**		210619/823
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0974. **CVE ID : CVE-2019-0909**	N/A	O-MIC-WIND-210619/824
Improper Input Validation	12-06-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0709, CVE-2019-0722. **CVE ID : CVE-2019-0620**	N/A	O-MIC-WIND-210619/825
Improper Input Validation	12-06-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka	N/A	O-MIC-WIND-210619/826

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
			'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0620, CVE-2019-0722. **CVE ID : CVE-2019-0709**		
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0711, CVE-2019-0713. **CVE ID : CVE-2019-0710**	N/A	O-MIC-WIND-210619/827
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0713. **CVE ID : CVE-2019-0711**	N/A	O-MIC-WIND-210619/828
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0711. **CVE ID : CVE-2019-0713**	N/A	O-MIC-WIND-210619/829
Improper Input Validatio	12-06-2019	9	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate	N/A	O-MIC-WIND-210619/830

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
n			input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0620, CVE-2019-0709. **CVE ID : CVE-2019-0722**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in the way that ActiveX Data Objects (ADO) handle objects in memory, aka 'ActiveX Data Objects (ADO) Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0888**	N/A	O-MIC-WIND-210619/831
N/A	12-06-2019	5	A denial of service exists in Microsoft IIS Server when the optional request filtering feature improperly handles requests, aka 'Microsoft IIS Server Denial of Service Vulnerability'. **CVE ID : CVE-2019-0941**	N/A	O-MIC-WIND-210619/832
N/A	12-06-2019	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'. **CVE ID : CVE-2019-0943**	N/A	O-MIC-WIND-210619/833
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists in the Windows Event Viewer	N/A	O-MIC-WIND-210619/834

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
			(eventvwr.msc) when it improperly parses XML input containing a reference to an external entity, aka 'Windows Event Viewer Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0948**		
N/A	12-06-2019	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'. This CVE ID is unique from CVE-2019-0984. **CVE ID : CVE-2019-0959**	N/A	O-MIC-WIND-210619/835
N/A	12-06-2019	6.8	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2019-0972**	N/A	O-MIC-WIND-210619/836
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-210619/837

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-2019-0973		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909. **CVE ID : CVE-2019-0974**	N/A	O-MIC-WIND-210619/838
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0998. **CVE ID : CVE-2019-0983**	N/A	O-MIC-WIND-210619/839
N/A	12-06-2019	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'. This CVE ID is unique from CVE-2019-0959. **CVE ID : CVE-2019-0984**	N/A	O-MIC-WIND-210619/840
N/A	12-06-2019	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of	N/A	O-MIC-WIND-210619/841

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 Vulnerability'. **CVE ID : CVE-2019-0986**		
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1012**	N/A	O-MIC-WIND-210619/842
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0983. **CVE ID : CVE-2019-0998**	N/A	O-MIC-WIND-210619/843
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1021, CVE-2019-1022, CVE-2019-1026, CVE-2019-1027, CVE-2019-1028. **CVE ID : CVE-2019-1007**	N/A	O-MIC-WIND-210619/844
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents	N/A	O-MIC-WIND-210619/845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1010**		
N/A	12-06-2019	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-2019-0960, CVE-2019-1017. **CVE ID : CVE-2019-1014**	N/A	O-MIC-WIND-210619/846
N/A	12-06-2019	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-2019-0960, CVE-2019-1014. **CVE ID : CVE-2019-1017**	N/A	O-MIC-WIND-210619/847
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1018**	N/A	O-MIC-WIND-210619/848
N/A	12-06-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign	N/A	O-MIC-WIND-210619/849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1019**		
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1022, CVE-2019-1026, CVE-2019-1027, CVE-2019-1028. **CVE ID : CVE-2019-1021**	N/A	O-MIC-WIND-210619/850
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1026, CVE-2019-1027, CVE-2019-1028. **CVE ID : CVE-2019-1022**	N/A	O-MIC-WIND-210619/851
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	7.8	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-1025**	N/A	O-MIC-WIND-210619/852
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege	N/A	O-MIC-WIND-210619/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1027, CVE-2019-1028. **CVE ID : CVE-2019-1026**		
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1026, CVE-2019-1028. **CVE ID : CVE-2019-1027**	N/A	O-MIC-WIND-210619/854
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1026, CVE-2019-1027. **CVE ID : CVE-2019-1028**	N/A	O-MIC-WIND-210619/855
Information Exposure	12-06-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1039**	N/A	O-MIC-WIND-210619/856
N/A	12-06-2019	4.3	A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows	N/A	O-MIC-WIND-210619/857

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
			NTLM Tampering Vulnerability'. **CVE ID : CVE-2019-1040**		
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1065. **CVE ID : CVE-2019-1041**	N/A	O-MIC-WIND-210619/858
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	8.5	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1043**	N/A	O-MIC-WIND-210619/859
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1046**	N/A	O-MIC-WIND-210619/860
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component	N/A	O-MIC-WIND-210619/861

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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049. **CVE ID : CVE-2019-1050**		
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows Shell fails to validate folder shortcuts, aka 'Windows Shell Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1053**	N/A	O-MIC-WIND-210619/862
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1064**	N/A	O-MIC-WIND-210619/863
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1041. **CVE ID : CVE-2019-1065**	N/A	O-MIC-WIND-210619/864
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the way the Task Scheduler Service validates	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
			certain file operations, aka 'Task Scheduler Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1069**		210619/865
windows_server_2019					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0904**	N/A	O-MIC-WIND-210619/866
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0905**	N/A	O-MIC-WIND-210619/867
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909,	N/A	O-MIC-WIND-210619/868

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-2019-0974. **CVE ID : CVE-2019-0906**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0908, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0907**	N/A	O-MIC-WIND-210619/869
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0909, CVE-2019-0974. **CVE ID : CVE-2019-0908**	N/A	O-MIC-WIND-210619/870
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0974. **CVE ID : CVE-2019-0909**	N/A	O-MIC-WIND-210619/871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-06-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0709, CVE-2019-0722. **CVE ID : CVE-2019-0620**	N/A	O-MIC-WIND-210619/872
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0711, CVE-2019-0713. **CVE ID : CVE-2019-0710**	N/A	O-MIC-WIND-210619/873
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-0710, CVE-2019-0713. **CVE ID : CVE-2019-0711**	N/A	O-MIC-WIND-210619/874
Improper Input Validation	12-06-2019	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'. This CVE ID is unique from CVE-2019-	N/A	O-MIC-WIND-210619/875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0710, CVE-2019-0711. **CVE ID : CVE-2019-0713**		
Improper Input Validation	12-06-2019	9	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0620, CVE-2019-0709. **CVE ID : CVE-2019-0722**	N/A	O-MIC-WIND-210619/876
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	9.3	A remote code execution vulnerability exists in the way that ActiveX Data Objects (ADO) handle objects in memory, aka 'ActiveX Data Objects (ADO) Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0888**	N/A	O-MIC-WIND-210619/877
N/A	12-06-2019	5	A denial of service exists in Microsoft IIS Server when the optional request filtering feature improperly handles requests, aka 'Microsoft IIS Server Denial of Service Vulnerability'. **CVE ID : CVE-2019-0941**	N/A	O-MIC-WIND-210619/878
N/A	12-06-2019	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	N/A	O-MIC-WIND-210619/879

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
			'Windows ALPC Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0943**		
Information Exposure	12-06-2019	4.3	An information disclosure vulnerability exists in the Windows Event Viewer (eventvwr.msc) when it improperly parses XML input containing a reference to an external entity, aka 'Windows Event Viewer Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0948**	N/A	O-MIC-WIND-210619/880
N/A	12-06-2019	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'. This CVE ID is unique from CVE-2019-0984. **CVE ID : CVE-2019-0959**	N/A	O-MIC-WIND-210619/881
N/A	12-06-2019	6.8	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2019-0972**	N/A	O-MIC-WIND-210619/882
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to	N/A	O-MIC-WIND-210619/883

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
			an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0973**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	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-2019-0904, CVE-2019-0905, CVE-2019-0906, CVE-2019-0907, CVE-2019-0908, CVE-2019-0909. **CVE ID : CVE-2019-0974**	N/A	O-MIC-WIND-210619/884
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0998. **CVE ID : CVE-2019-0983**	N/A	O-MIC-WIND-210619/885
N/A	12-06-2019	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'. This CVE ID is unique from CVE-2019-0959. **CVE ID : CVE-2019-0984**	N/A	O-MIC-WIND-210619/886

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
N/A	12-06-2019	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0986**	N/A	O-MIC-WIND-210619/887
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1012**	N/A	O-MIC-WIND-210619/888
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0983. **CVE ID : CVE-2019-0998**	N/A	O-MIC-WIND-210619/889
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1021, CVE-2019-1022, CVE-2019-1026,	N/A	O-MIC-WIND-210619/890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-1027, CVE-2019-1028. **CVE ID : CVE-2019-1007**		
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1010**	N/A	O-MIC-WIND-210619/891
N/A	12-06-2019	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-2019-0960, CVE-2019-1017. **CVE ID : CVE-2019-1014**	N/A	O-MIC-WIND-210619/892
N/A	12-06-2019	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-2019-0960, CVE-2019-1014. **CVE ID : CVE-2019-1017**	N/A	O-MIC-WIND-210619/893
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation	N/A	O-MIC-WIND-210619/894

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 Privilege Vulnerability'. **CVE ID : CVE-2019-1018**		
N/A	12-06-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1019**	N/A	O-MIC-WIND-210619/895
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1022, CVE-2019-1026, CVE-2019-1027, CVE-2019-1028. **CVE ID : CVE-2019-1021**	N/A	O-MIC-WIND-210619/896
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1026, CVE-2019-1027, CVE-2019-1028. **CVE ID : CVE-2019-1022**	N/A	O-MIC-WIND-210619/897
Improper Restriction of Operations within the Bounds of a	12-06-2019	7.8	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-1025**	N/A	O-MIC-WIND-210619/898

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					
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1027, CVE-2019-1028. **CVE ID : CVE-2019-1026**	N/A	O-MIC-WIND-210619/899
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1026, CVE-2019-1028. **CVE ID : CVE-2019-1027**	N/A	O-MIC-WIND-210619/900
N/A	12-06-2019	4.6	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1007, CVE-2019-1021, CVE-2019-1022, CVE-2019-1026, CVE-2019-1027. **CVE ID : CVE-2019-1028**	N/A	O-MIC-WIND-210619/901
Information Exposure	12-06-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-210619/902

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-2019-1039		
N/A	12-06-2019	4.3	A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'. **CVE ID : CVE-2019-1040**	N/A	O-MIC-WIND-210619/903
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1065. **CVE ID : CVE-2019-1041**	N/A	O-MIC-WIND-210619/904
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-06-2019	8.5	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1043**	N/A	O-MIC-WIND-210619/905
N/A	12-06-2019	7.2	A security feature bypass vulnerability exists when Windows Secure Kernel Mode fails to properly handle objects in memory.To exploit the vulnerability, a locally-authenticated attacker could attempt to run a specially crafted application on a targeted system, aka 'Windows Secure Kernel Mode Security Feature Bypass	N/A	O-MIC-WIND-210619/906

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-2019-1044**		
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050. **CVE ID : CVE-2019-1046**	N/A	O-MIC-WIND-210619/907
Information Exposure	12-06-2019	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-2019-0968, CVE-2019-0977, CVE-2019-1009, CVE-2019-1010, CVE-2019-1011, CVE-2019-1012, CVE-2019-1013, CVE-2019-1015, CVE-2019-1016, CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1049. **CVE ID : CVE-2019-1050**	N/A	O-MIC-WIND-210619/908
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows Shell fails to validate folder shortcuts, aka 'Windows Shell Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1053**	N/A	O-MIC-WIND-210619/909

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
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1064**	N/A	O-MIC-WIND-210619/910
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1041. **CVE ID : CVE-2019-1065**	N/A	O-MIC-WIND-210619/911
N/A	12-06-2019	7.2	An elevation of privilege vulnerability exists in the way the Task Scheduler Service validates certain file operations, aka 'Task Scheduler Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1069**	N/A	O-MIC-WIND-210619/912
Opensuse					
leap					
N/A	11-06-2019	5	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them. **CVE ID : CVE-2019-0220**	N/A	O-OPE-LEAP-210619/913

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
pix-link					
lv-wr09_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-06-2019	4.3	XSS on the PIX-Link Repeater/Router LV-WR09 with firmware v28K.MiniRouter.20180616 allows attackers to steal credentials without being connected to the network. The attack vector is a crafted ESSID. **CVE ID : CVE-2019-11877**	N/A	O-PIX-LV-W-210619/914
Redhat					
virtualization					
N/A	12-06-2019	5	A vulnerability was found in Undertow web server before 2.0.21. An information exposure of plain text credentials through log files because Connectors.executeRootHandler: 402 logs the HttpServerExchange object at ERROR level using UndertowLogger.REQUEST_LOGGER.undertowRequestFailed(t, exchange) **CVE ID : CVE-2019-3888**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3888	O-RED-VIRT-210619/915
enterprise_linux					
N/A	07-06-2019	5	A security regression of CVE-2019-9636 was discovered in python since commit d537ab0ff9767ef024f26246899728f0116b1ec3 affecting versions 2.7, 3.5, 3.6, 3.7 and from v3.8.0a4 through v3.8.0b1, which still allows an attacker to exploit CVE-2019-9636 by abusing the user and password parts of a URL. When an application parses	N/A	O-RED-ENTE-210619/916

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
			user-supplied URLs to store cookies, authentication credentials, or other kind of information, it is possible for an attacker to provide specially crafted URLs to make the application locate host-related information (e.g. cookies, authentication data) and send them to a different host than where it should, unlike if the URLs had been correctly parsed. The result of an attack may vary based on the application. **CVE ID : CVE-2019-10160**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-06-2019	8.3	A flaw that allowed an attacker to corrupt memory and possibly escalate privileges was found in the mwifiex kernel module while connecting to a malicious wireless network. **CVE ID : CVE-2019-3846**	N/A	O-RED-ENTE-210619/917
Samsung					
galaxy_s4_firmware					
N/A	06-06-2019	1.9	Xiaomi Mi 5s Plus devices allow attackers to trigger touchscreen anomalies via a radio signal between 198 kHz and 203 kHz, as demonstrated by a transmitter and antenna hidden just beneath the surface of a coffee-shop table, aka Ghost Touch. **CVE ID : CVE-2019-12762**	N/A	O-SAM-GALA-210619/918
galaxy_s6_edge_firmware					
N/A	06-06-2019	1.9	Xiaomi Mi 5s Plus devices allow attackers to trigger touchscreen	N/A	O-SAM-GALA-

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
			anomalies via a radio signal between 198 kHz and 203 kHz, as demonstrated by a transmitter and antenna hidden just beneath the surface of a coffee-shop table, aka Ghost Touch. **CVE ID : CVE-2019-12762**		210619/919
Sharp					
aquos_zeta_sh-04f_firmware					
N/A	06-06-2019	1.9	Xiaomi Mi 5s Plus devices allow attackers to trigger touchscreen anomalies via a radio signal between 198 kHz and 203 kHz, as demonstrated by a transmitter and antenna hidden just beneath the surface of a coffee-shop table, aka Ghost Touch. **CVE ID : CVE-2019-12762**	N/A	O-SHA-AQUO-210619/920
Sony					
xperia_z4_firmware					
N/A	06-06-2019	1.9	Xiaomi Mi 5s Plus devices allow attackers to trigger touchscreen anomalies via a radio signal between 198 kHz and 203 kHz, as demonstrated by a transmitter and antenna hidden just beneath the surface of a coffee-shop table, aka Ghost Touch. **CVE ID : CVE-2019-12762**	N/A	O-SON-XPER-210619/921
soyal					
ar-727h_firmware					
Improper Authentication	06-06-2019	5	On SOYAL AR-727H and AR-829Ev5 devices, all CGI programs allow unauthenticated POST access. **CVE ID : CVE-2019-6451**	N/A	O-SOY-AR-7-210619/922

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
ar-829ev5_firmware					
Improper Authentication	06-06-2019	5	On SOYAL AR-727H and AR-829Ev5 devices, all CGI programs allow unauthenticated POST access. **CVE ID : CVE-2019-6451**	N/A	O-SOY-AR-8-210619/923
supra					
stv-lc40lt0020f_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-06-2019	2.1	Supra Smart Cloud TV allows remote file inclusion in the openLiveURL function, which allows a local attacker to broadcast fake video without any authentication via a /remote/media_control?action=setUri&uri= URI. **CVE ID : CVE-2019-12477**	N/A	O-SUP-STV--210619/924
Tp-link					
tl-wr940n_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-06-2019	9	TP-Link TL-WR940N is vulnerable to a stack-based buffer overflow, caused by improper bounds checking by the ipAddrDispose function. By sending specially crafted ICMP echo request packets, a remote authenticated attacker could overflow a buffer and execute arbitrary code on the system with elevated privileges. **CVE ID : CVE-2019-6989**	N/A	O-TP--TL-W-210619/925
tl-wr941nd_firmware					
Improper Restriction of Operatio	06-06-2019	9	TP-Link TL-WR940N is vulnerable to a stack-based buffer overflow, caused by improper bounds checking by the	N/A	O-TP--TL-W-210619/926

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
ns within the Bounds of a Memory Buffer			ipAddrDispose function. By sending specially crafted ICMP echo request packets, a remote authenticated attacker could overflow a buffer and execute arbitrary code on the system with elevated privileges. **CVE ID : CVE-2019-6989**		
tzumi					
klic_smart_padlock_model_5686_firmware					
Improper Authentication	11-06-2019	4.3	An authentication bypass in website post requests in the Tzumi Electronics Klic Lock application 1.0.9 for mobile devices allows attackers to access resources (that are not otherwise accessible without proper authentication) via capture-replay. Physically proximate attackers can use this information to unlock unauthorized Tzumi Electronics Klic Smart Padlock Model 5686 Firmware 6.2. **CVE ID : CVE-2019-11334**	N/A	O-TZU-KLIC-210619/927
ui					
aircam_firmware					
Improper Input Validation	04-06-2019	7.8	On Ubiquiti airCam 3.1.4 devices, a Denial of Service vulnerability exists in the RTSP Service provided by the ubnt-streamer binary. The issue can be triggered via malformed RTSP requests that lead to an invalid memory read. To exploit the vulnerability, an attacker must craft an RTSP request with a large number of headers.	N/A	O-UI-AIRC-210619/928

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-2019-12727		
Xiaomi					
mi_5s_plus_firmware					
N/A	06-06-2019	1.9	Xiaomi Mi 5s Plus devices allow attackers to trigger touchscreen anomalies via a radio signal between 198 kHz and 203 kHz, as demonstrated by a transmitter and antenna hidden just beneath the surface of a coffee-shop table, aka Ghost Touch. **CVE ID : CVE-2019-12762**	N/A	O-XIA-MI_5-210619/929
ZTE					
netnumen_dap_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-06-2019	3.5	All versions up to V20.18.40.R7.B1of ZTE NetNumen DAP product have an XSS vulnerability. Due to the lack of correct validation of client data in WEB applications, which results in users being hijacked. **CVE ID : CVE-2019-3413**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1010797	O-ZTE-NETN-210619/930