Vulnerability Summary for the Week of June 10, 2019

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by Ug-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of Ug-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- coldfusion	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.	2019-06-12	10.0	CVE-2019-7838 CONFIRM
adobe -- coldfusion	ColdFusion versions Update 3 and earlier, Update 10 and earlier, and Update 18 and earlier have a command injection vulnerability. Successful exploitation	2019-06-12	10.0	CVE-2019-7839 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could lead to arbitrary code execution.			
adobe -- coldfusion	ColdFusion versions Update 3 and earlier, Update 10 and earlier, and Update 18 and earlier have a deserialization of untrusted data vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-06-12	10.0	CVE-2019-7840 CONFIRM
apache -- fineract	SQL injection vulnerability in Apache Fineract before 1.3.0 allows attackers to execute arbitrary SQL commands via a query on the GroupSummaryCounts related table.	2019-06-11	7.5	CVE-2018-11800 MLIST BID MLIST
apache -- fineract	SQL injection vulnerability in Apache Fineract before 1.3.0 allows attackers to execute arbitrary SQL commands via a query on a m_center data related table.	2019-06-11	7.5	CVE-2018-11801 MLIST BID MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
artifex -- mujs	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.	2019-06-13	7.5	CVE-2019-12798 MISC
artifex -- mupdf	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.	2019-06-13	7.5	CVE-2019-7321 MISC
aubio -- aubio	aubio v0.4.0 to v0.4.8 has a Buffer Overflow (issue 1 of 3).	2019-06-07	7.5	CVE-2018-19800 MISC
cesanta -- mongoose	An invalid read of 8 bytes due to a use-after-free vulnerability during a "NULL test" in the mg_http_get_proto_data function in mongoose.c in Cesanta Mongoose Embedded Web Server Library 6.13 and earlier allows a denial of service (application crash) or remote code execution.	2019-06-10	7.5	CVE-2018-20353 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cesanta -- mongoose	An invalid read of 8 bytes due to a use-after-free vulnerability during a "return" in the mg_http_get_proto_data function in mongoose.c in Cesanta Mongoose Embedded Web Server Library 6.13 and earlier allows a denial of service (application crash) or remote code execution.	2019-06-10	7.5	CVE-2018-20354 MISC
cesanta -- mongoose	An invalid write of 8 bytes due to a use-after-free vulnerability in the mg_http_free_proto_data_cgi function call in mongoose.c in Cesanta Mongoose Embedded Web Server Library 6.13 and earlier allows a denial of service (application crash) or remote code execution.	2019-06-10	7.5	CVE-2018-20355 MISC
cesanta -- mongoose	An invalid read of 8 bytes due to a use-after-free vulnerability in the mg_http_free_proto_data_cgi function call in mongoose.c in Cesanta Mongoose Embedded Web Server Library 6.13 and earlier allows a denial of service (application crash) or remote code execution.	2019-06-10	7.5	CVE-2018-20356 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dlink -- dir-300_firmware	An issue was discovered in soap.cgi?service=WANIPConn1 on D-Link DIR-845 before v1.02b03, DIR-600 before v2.17b01, DIR-645 before v1.04b11, DIR-300 rev. B, and DIR-865 devices. There is Command Injection via shell metacharacters in the NewInternalClient, NewExternalPort, or NewInternalPort element of a SOAP POST request.	2019-06-11	7.5	CVE-2013-7471 MISC MISC
enttec -- datagate_mk2_firmware	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	2019-06-07	9.0	CVE-2019-12775 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	possible for a threat actor to create or run high-privileged binaries or executables that are available within the operating system of the device.)			
enttec -- datagate_mk2_firmware	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.	2019-06-07	10.0	CVE-2019-12776 MISC
enttec -- datagate_mk2_firmware	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	2019-06-07	7.2	CVE-2019-12777 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
goahead -- wireless_ip_camere_wificam_firmware	An issue was discovered on Wireless IP Camera (P2P) WIFICAM cameras. There is Command Injection in the set_ftp.cgi script via shell metacharacters in the pwd variable, as demonstrated by a set_ftp.cgi?svr=192.168.1.1&port=21&user=ftp URI.	2019-06-11	10.0	CVE-2017-18377 MISC
google -- android	In GetPermittedAccessibilityServicesForUser of DevicePolicyManagerService.java, there is a possible	2019-06-07	7.2	CVE-2019-2091 CON

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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 ID: A-128599660.			FIRM
google -- android	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.	2019-06-07	7.2	CVE-2019-2092 CONFIRM
google -- android	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	2019-06-07	9.3	CVE-2019-2093 CON

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-119292397.			FIRM
google -- android	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.	2019-06-07	9.3	CVE-2019-2094 CONFIRM
google -- android	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:	2019-06-07	7.6	CVE-2019-2095 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Android. Versions: Android-9. Android ID: A-124232283.			
google -- android	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-123237974.	2019-06-07	7.2	CVE-2019-2096 CONFIRM
google -- android	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-	2019-06-07	10.0	CVE-2019-2097 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	8.1 Android-9. Android ID: A-117606285.			
google -- android	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.	2019-06-07	7.2	CVE-2019-2098 CONFIRM
google -- android	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 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-	2019-06-07	9.3	CVE-2019-2099 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	8.1 Android-9. Android ID: A-123583388.			
google -- android	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.	2019-06-07	8.3	CVE-2019-2102 CONFIRM
hootoo -- tripmate_titan_ht-tm05_firmware	HooToo TripMate Titan HT-TM05 and HT-05 routers with firmware 2.000.022 and 2.000.082 allow remote command execution via shell metacharacters in the mac parameter of a protocol.csp?function=set&fname=security&opt=mac_table request.	2019-06-11	10.0	CVE-2018-20841 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hoteldruid -- hoteldruid	HotelDruid before v2.3.1 has SQL Injection via the /visualizza_tabelle.php anno parameter.	2019-06-07	7.5	CVE-2019-9086 MISC MISC
hoteldruid -- hoteldruid	HotelDruid before v2.3.1 has SQL Injection via the /tab_tariffe.php numtariffa1 parameter.	2019-06-07	7.5	CVE-2019-9087 MISC MISC
ipswitch -- ws_ftp_server	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.	2019-06-11	7.5	CVE-2019-12144 CONFIRM
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.7. The CSV export of com_actionslogs is vulnerable to CSV injection.	2019-06-11	7.5	CVE-2019-12765 BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC
logitech -- r700_laser_presentation_remote_firmware	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.	2019-06-07	8.3	CVE-2019-12506 MISC FULLDISC BUGTRAQ MISC
microsoft -- chakracore	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-	2019-06-12	7.6	CVE-2019-0989 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2019-1024, CVE-2019-1051, CVE-2019-1052.			
microsoft -- chakracore	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, CVE-2019-1051, CVE-2019-1052.	2019-06-12	7.6	CVE-2019-0991 MISC
microsoft -- chakracore	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.	2019-06-12	7.6	CVE-2019-0993 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- chakracore	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.	2019-06-12	7.6	CVE-2019-1003 MISC
microsoft -- chakracore	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.	2019-06-12	7.6	CVE-2019-1024 MISC
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles	2019-06-12	7.6	CVE-2019-1051

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			MISC
microsoft -- chakracore	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.	2019-06-12	7.6	CVE-2019-1052 MISC
microsoft -- edge	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'.	2019-06-12	7.6	CVE-2019-0992 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
microsoft -- edge	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, CVE-2019-1051, CVE-2019-1052.	2019-06-12	7.6	CVE-2019-1002 MISC
microsoft -- edge	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'.	2019-06-12	7.6	CVE-2019-1038 MISC
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way the scripting engine	2019-06-12	7.6	CVE-2019-0920

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			MISC
microsoft -- internet_explorer	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.	2019-06-12	7.6	CVE-2019-0988 MISC
microsoft -- internet_explorer	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-2019-1055, CVE-2019-1080.	2019-06-12	7.6	CVE-2019-1005 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- internet_explorer	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.	2019-06-12	7.6	CVE-2019-1055 MISC
microsoft -- internet_explorer	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.	2019-06-12	7.6	CVE-2019-1080 MISC
microsoft -- lync_server	A denial of service vulnerability exists in Skype for Business, aka 'Skype for Business and Lync Server Denial of Service Vulnerability'.	2019-06-12	7.1	CVE-2019-1029 MISC
microsoft -- office	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly	2019-06-12	9.3	CVE-2019-1034

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1035.			MISC
microsoft -- office	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.	2019-06-12	9.3	CVE-2019-1035 MISC MISC
microsoft -- windows_10	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.	2019-06-12	7.7	CVE-2019-0620 MISC
microsoft -- windows_10	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly	2019-06-12	7.7	CVE-2019-0709

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			MISC
microsoft -- windows_10	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.	2019-06-12	9.0	CVE-2019-0722 MISC
microsoft -- windows_10	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'.	2019-06-12	9.3	CVE-2019-0888 MISC
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles	2019-06-12	9.3	CVE-2019-0904

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			MISC
microsoft -- windows_10	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.	2019-06-12	9.3	CVE-2019-0905 MISC
microsoft -- windows_10	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-	2019-06-12	9.3	CVE-2019-0906 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2019-0908, CVE-2019-0909, CVE-2019-0974.			
microsoft -- windows_10	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.	2019-06-12	9.3	CVE-2019-0907 MISC
microsoft -- windows_10	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.	2019-06-12	9.3	CVE-2019-0908 MISC
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles	2019-06-12	9.3	CVE-2019-0909

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			MISC
microsoft -- windows_10	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'.	2019-06-12	7.2	CVE-2019-0943 MISC
microsoft -- windows_10	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.	2019-06-12	7.2	CVE-2019-0959 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	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'.	2019-06-12	7.2	CVE-2019-0973 MISC
microsoft -- windows_10	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.	2019-06-12	9.3	CVE-2019-0974 MISC
microsoft -- windows_10	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	2019-06-12	7.2	CVE-2019-0983 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	is unique from CVE-2019-0998.			
microsoft -- windows_10	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.	2019-06-12	7.2	CVE-2019-0984 MISC
microsoft -- windows_10	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.	2019-06-12	7.2	CVE-2019-0998 MISC
microsoft -- windows_10	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.	2019-06-12	7.2	CVE-2019-1014 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	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.	2019-06-12	7.2	CVE-2019-1017 MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'.	2019-06-12	7.2	CVE-2019-1018 MISC
microsoft -- windows_10	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'.	2019-06-12	7.8	CVE-2019-1025 MISC
microsoft -- windows_10	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.	2019-06-12	7.2	CVE-2019-1041 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'.	2019-06-12	8.5	CVE-2019-1043 MISC
microsoft -- windows_10	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'.	2019-06-12	7.2	CVE-2019-1044 MISC
microsoft -- windows_10	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'.	2019-06-12	7.2	CVE-2019-1045 MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists when the Windows Shell fails to validate folder shortcuts, aka	2019-06-12	7.2	CVE-2019-1053

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	'Windows Shell Elevation of Privilege Vulnerability'.			MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'.	2019-06-12	7.2	CVE-2019-1064 MISC
microsoft -- windows_10	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.	2019-06-12	7.2	CVE-2019-1065 MISC MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in the way the Task Scheduler Service validates certain file operations, aka 'Task Scheduler Elevation of Privilege Vulnerability'.	2019-06-12	7.2	CVE-2019-1069 MISC MISC CERT-VN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_7	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.	2019-06-12	7.2	CVE-2019-0960 MISC
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.14 devices. The Moxa AWK 3121 provides ping functionality so that an administrator can execute ICMP calls to check if the network is working correctly. However, the same functionality allows an attacker to execute commands on the device. The POST parameter "srvName" is susceptible to this injection. By crafting a packet that contains shell metacharacters, it is possible for an attacker to execute the attack.	2019-06-07	9.3	CVE-2018-10697 MISC MISC BUGTRAQ
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.14 devices. The device enables an unencrypted TELNET service by default. This	2019-06-07	10.0	CVE-2018-10698 MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows an attacker who has been able to gain an MITM position to easily sniff the traffic between the device and the user. Also an attacker can easily connect to the TELNET daemon using the default credentials if they have not been changed by the user.			CONFIRM BUGTRAQ
openid -- ruby-openid	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.	2019-06-10	10.0	CVE-2019-11027 MISC MISC
salesagility -- suitecrm	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).	2019-06-07	7.5	CVE-2019-12598 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
salesagility -- suitecrm	SuiteCRM 7.10.x before 7.10.17 and 7.11.x before 7.11.5 allows SQL Injection.	2019-06-07	7.5	CVE-2019-12599 CONFIRM
salesagility -- suitecrm	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).	2019-06-07	7.5	CVE-2019-12600 CONFIRM
salesagility -- suitecrm	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).	2019-06-07	7.5	CVE-2019-12601 CONFIRM
sap -- advanced_business_application_programming_platform_kernel	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,	2019-06-12	7.5	CVE-2019-0304 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
seowonintech -- swr-300a_firmware	On Seowon Intech routers, there is a Command Injection vulnerability in diagnostic.cgi via shell metacharacters in the ping_ipaddr parameter.	2019-06-11	10.0	CVE-2016-10760 MISC
solarwinds -- serv-u_ftp_server	The local management interface in SolarWinds Serv-U FTP Server 15.1.6.25 has incorrect access controls that permit local users to bypass authentication in the application and execute code in the context of the Windows SYSTEM account, leading to privilege escalation. To exploit this vulnerability, an attacker must have local access the the host running Serv-U, and a Serv-U administrator have an active management console session.	2019-06-07	7.2	CVE-2018-19999 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
thinstation_project -- thinstation	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.	2019-06-07	7.5	CVE-2019-12771 MISC
veracomp -- asmax_ar-804gu_firmware	An issue was discovered on ASMAX AR-804gu 66.34.1 devices. There is Command Injection via the cgi-bin/script query string.	2019-06-11	10.0	CVE-2009-5156 MISC MISC
wpgraphql -- wpgraphql	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.	2019-06-10	7.5	CVE-2019-9879 MISC MISC CONFIRM MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- flash_player	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.	2019-06-12	6.8	CVE-2019-7845 CONFIRM
apache -- http_server	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.	2019-06-11	5.0	CVE-2019-0196 SUSE SUSE SUSE MISC MLIST BID CONFIRM MLIST MLIST FEDORA FEDORA BUGTRAQ CONFIRM UBU

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				NTU DEBIAN
apache -- http_server	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.	2019-06-11	4.9	CVE-2019-0197 SUSE SUSE SUSE MLIST BID CONFIRM MISC FEDORA CONFIRM
apache -- http_server	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.	2019-06-11	5.0	CVE-2019-0220 SUSE SUSE SUSE MLIST BID CONFIRM MLIST FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				FEDORA FEDORA BUGTRAQ CONFIRM UBUNTU DEBIAN
aubio -- aubio	aubio v0.4.0 to v0.4.8 has a NULL pointer dereference (issue 1 of 6).	2019-06-07	5.0	CVE-2018-19801 MISC
aubio -- aubio	aubio v0.4.0 to v0.4.8 has a Buffer Overflow (issue 2 of 3).	2019-06-07	5.0	CVE-2018-19802 MISC
bevywise -- mqttroute	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.	2019-06-10	5.0	CVE-2019-6241 MISC
broadcom -- bcm4335c0_firmware	Broadcom firmware before summer 2014 on Nexus 5 BCM4335C0 2012-12-11,	2019-06-07	5.8	CVE-2018-19860

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Raspberry Pi 3 BCM43438A1 2014-06-02, and unspecifed other devices does not properly restrict LMP commnds and executes certain memory contents upon receiving an LMP command, as demonstrated by executing an HCI command.			CONFIRM MISC
cesanta -- mongoose_embedded_web_server_library	Use-after-free vulnerability in the mg_cgi_ev_handler function in mongoose.c in Cesanta Mongoose Embedded Web Server Library 6.13 and earlier allows a denial of service (application crash) or remote code execution.	2019-06-10	6.8	CVE-2018-20352 MISC
cloudera -- cloudera_manager	This CVE relates to an unspecified cross site scripting vulnerability in Cloudera Manager.	2019-06-07	4.3	CVE-2018-5798 MISC CONFIRM
cloudera -- cloudera_manager	In Cloudera Navigator Key Trustee KMS 5.12 and 5.13, incorrect default ACL values allow remote access to purge and undelete API calls on encryption zone keys. The Navigator Key Trustee KMS includes 2 API calls in addition to those in Apache Hadoop KMS: purge and undelete. The KMS ACL values for these commands are	2019-06-07	5.5	CVE-2018-6185 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	keytrustee.kms.acl.PURGE and keytrustee.kms.acl.UNDELETE respectively. The default value for the ACLs in Key Trustee KMS 5.12.0 and 5.13.0 is "*" which allows anyone with knowledge of the name of an encryption zone key and network access to the Key Trustee KMS to make those calls against known encryption zone keys. This can result in the recovery of a previously deleted, but not purged, key (undelete) or the deletion of a key in active use (purge) resulting in loss of access to encrypted HDFS data.			
cloudera -- data_science_workbench	An SQL injection vulnerability was found in Cloudera Data Science Workbench (CDSW) 1.4.0 through 1.4.2. This would allow any authenticated user to run arbitrary queries against CDSW's internal database. The database contains user contact information, encrypted CDSW passwords (in the case of local authentication), API keys, and stored Kerberos keytabs.	2019-06-07	6.5	CVE-2018-20091 CONFIRM MISC
clusterlabs -- libqb	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.	2019-06-07	6.6	CVE-2019-12779 BID MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
dameware -- remote_mini_control	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.	2019-06-07	5.0	CVE-2019-3955 MISC
dameware -- remote_mini_control	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 information.	2019-06-07	5.8	CVE-2019-3956 MISC
dameware -- remote_mini_control	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.	2019-06-07	5.8	CVE-2019-3957 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dlink -- dir-818lw_firmware	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.	2019-06-10	6.5	CVE-2019-12786 MISC
dlink -- dir-818lw_firmware	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.	2019-06-10	6.5	CVE-2019-12787 MISC
enttec -- datagate_mk2_firmware	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.	2019-06-07	4.3	CVE-2019-12774 MISC
fatfreecrm -- fat_free_crm	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.	2019-06-10	4.3	CVE-2019-10226 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxitsoftware -- foxit_pdf_sdk_activex	A command injection can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031 when using the Open File action on a Field. An attacker can leverage this to gain remote code execution.	2019-06-07	6.8	CVE-2018-19451 BID MISC
foxitsoftware -- foxit_pdf_sdk_activex	A use after free in the TextBox field Mouse Enter action in IReader_ContentProvider can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031. An attacker can leverage this to gain remote code execution. Relative to CVE-2018-19444, this has a different free location and requires different JavaScript code for exploitation.	2019-06-07	6.8	CVE-2018-19452 BID MISC
fujielectric -- v-server	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 message handling logic.	2019-06-12	5.0	CVE-2019-3946 BID MISC
fujielectric -- v-server	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	2019-06-12	5.0	CVE-2019-3947 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	database credentials and gain access to the database server.			
gnome -- gvfs	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.)	2019-06-11	4.6	CVE-2019-12795 BID MISC MISC MISC
google -- android	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	2019-06-07	4.6	CVE-2019-2090 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	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.	2019-06-07	4.9	CVE-2019-2101 CONFIRM
hoteldruid -- hoteldruid	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).	2019-06-07	4.0	CVE-2019-9084 MISC MISC
huawei -- hg255s_firmware	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.	2019-06-10	4.3	CVE-2019-5243 MISC
huawei -- hisuite	HiSuite 9.1.0.300 versions and earlier contains a DLL hijacking vulnerability. This vulnerability	2019-06-13	4.6	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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 arbitrary code.			5245 MISC
ibm -- intelligent_operations_center	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.	2019-06-07	6.5	CVE-2019-4066 XF CONFIRM
ibm -- intelligent_operations_center	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.	2019-06-07	5.0	CVE-2019-4067 XF CONFIRM
ibm -- intelligent_operations_center	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.	2019-06-07	5.0	CVE-2019-4068 XF CONFIRM
ibm -- intelligent_operations_center	IBM Intelligent Operations Center (IOC) 5.1.0 through 5.2.0 does not properly validate file types, allowing an attacker to upload	2019-06-07	6.5	CVE-2019-4069 XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	malicious content. IBM X-Force ID: 157014.			CONFIRM
intel -- open_cloud_integrity_tehnology	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access.	2019-06-13	4.6	CVE-2019-0181 MISC
intel -- turbo_boost_max_technology_3.0	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.	2019-06-13	4.4	CVE-2019-0164 MISC MISC
ipswitch -- ws_ftp_server	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.	2019-06-11	5.0	CVE-2019-12143 CONFIRM
ipswitch -- ws_ftp_server	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	2019-06-11	5.0	CVE-2019-12145 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disclose path names on the host operating system.			
ipswitch -- ws_ftp_server	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.	2019-06-11	6.4	CVE-2019-12146 CONFIRM
jenkins -- electricflow	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.	2019-06-11	4.3	CVE-2019-10331 MLIST BID MISC
jenkins -- electricflow	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.	2019-06-11	4.3	CVE-2019-10332 MLIST BID MISC
jenkins -- electricflow	Missing permission checks in Jenkins ElectricFlow Plugin 1.1.5 and earlier in various HTTP	2019-06-11	4.0	CVE-2019-10333

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	endpoints allowed users with Overall/Read access to obtain information about the Jenkins ElectricFlow Plugin configuration and configuration of connected ElectricFlow instances.			MLIST BID MISC
jenkins -- electricflow	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.	2019-06-11	5.8	CVE-2019-10334 MLIST BID MISC
jenkins -- electricflow	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.	2019-06-11	4.3	CVE-2019-10336 MLIST BID MISC
jenkins -- jx_resources	A cross-site request forgery 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	2019-06-11	6.8	CVE-2019-10338 MLIST BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	server, potentially leaking credentials.			
jenkins -- jx_resources	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.	2019-06-11	4.0	CVE-2019-10339 MLIST BID MISC
jenkins -- token_macro	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.	2019-06-11	5.0	CVE-2019-10337 MLIST BID MISC
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.7. The update server URL of com_joomlaupdate can be manipulated by non Super-Admin users.	2019-06-11	4.0	CVE-2019-12764 BID MISC
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.7. The subform fieldtype does not sufficiently	2019-06-11	4.3	CVE-2019-12766

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	filter or validate input of subfields. This leads to XSS attack vectors.			BID MISC
maccms -- maccms	Maccms through 8.0 allows XSS via the site_keywords field to index.php?m=system-config because of tpl/module/system.php and tpl/html/system_config.html, related to template/paody/html/vod_index.html.	2019-06-07	4.3	CVE-2018-19465 MISC MISC
mi -- stock_browser	Xiaomi Stock Browser 10.2.4.g on Xiaomi Redmi Note 5 Pro devices and other Redmi Android phones allows content provider injection. In other words, a third-party application can read the user's cleartext browser history via an app.provider.query content://com.android.browser.searchhistory/searchhistory request.	2019-06-07	5.0	CVE-2018-20523 MISC MISC
microfocus -- solutions_business_manager	Micro Focus Solution Business Manager versions prior to 11.4.2 is susceptible to open redirect.	2019-06-07	5.8	CVE-2019-3477 CONFIRM
microsoft -- azure_devops_server_2019	A spoofing vulnerability exists in Azure DevOps Server when it improperly handles requests to authorize applications, resulting in a cross-site request forgery, aka	2019-06-12	4.3	CVE-2019-0996 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	'Azure DevOps Server Spoofing Vulnerability'.			
microsoft -- chakracore	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.	2019-06-12	4.3	CVE-2019-0990 MISC
microsoft -- chakracore	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.	2019-06-12	4.3	CVE-2019-1023 MISC
microsoft -- edge	A security feature bypass vulnerability exists in Edge that allows for bypassing Mark of the Web Tagging (MOTW), aka 'Microsoft Edge Security Feature Bypass Vulnerability'.	2019-06-12	5.1	CVE-2019-1054 MISC
microsoft -- edge	An information disclosure vulnerability exists when affected Microsoft browsers improperly handle objects in memory, aka 'Microsoft Browser Information Disclosure Vulnerability'.	2019-06-12	4.3	CVE-2019-1081 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	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.	2019-06-12	5.5	CVE-2019-0710 MISC
microsoft -- windows_10	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.	2019-06-12	5.5	CVE-2019-0711 MISC
microsoft -- windows_10	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.	2019-06-12	5.5	CVE-2019-0713 MISC
microsoft -- windows_10	A denial of service exists in Microsoft IIS Server when the optional request filtering feature improperly handles requests, aka	2019-06-12	5.0	CVE-2019-0941 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	'Microsoft IIS Server Denial of Service Vulnerability'.			
microsoft -- windows_10	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'.	2019-06-12	4.3	CVE-2019-0948 MISC
microsoft -- windows_10	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'.	2019-06-12	6.8	CVE-2019-0972 MISC
microsoft -- windows_10	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.	2019-06-12	4.6	CVE-2019-1007 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	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.	2019-06-12	4.3	CVE-2019-1010 MISC
microsoft -- windows_10	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.	2019-06-12	4.3	CVE-2019-1012 MISC
microsoft -- windows_10	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	2019-06-12	6.5	CVE-2019-1019 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'.			
microsoft -- windows_10	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.	2019-06-12	4.6	CVE-2019-1021 MISC
microsoft -- windows_10	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.	2019-06-12	4.6	CVE-2019-1022 MISC
microsoft -- windows_10	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.	2019-06-12	4.6	CVE-2019-1026 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	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.	2019-06-12	4.6	CVE-2019-1027 MISC
microsoft -- windows_10	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.	2019-06-12	4.6	CVE-2019-1028 MISC
microsoft -- windows_10	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'.	2019-06-12	4.3	CVE-2019-1040 MISC
microsoft -- windows_10	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,	2019-06-12	4.3	CVE-2019-1046 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
microsoft -- windows_10	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.	2019-06-12	4.3	CVE-2019-1050 MISC
microsoft -- windows_7	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.	2019-06-12	4.3	CVE-2019-0968 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_7	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.	2019-06-12	4.3	CVE-2019-0977 MISC
microsoft -- windows_7	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'.	2019-06-12	6.8	CVE-2019-0985 MISC
microsoft -- windows_7	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,	2019-06-12	4.3	CVE-2019-1009 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVE-2019-1047, CVE-2019-1048, CVE-2019-1049, CVE-2019-1050.			
microsoft -- windows_7	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.	2019-06-12	4.3	CVE-2019-1011 MISC
microsoft -- windows_7	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.	2019-06-12	4.3	CVE-2019-1013 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_7	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.	2019-06-12	4.3	CVE-2019-1015 MISC
microsoft -- windows_7	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.	2019-06-12	4.3	CVE-2019-1016 MISC
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure	2019-06-12	4.3	CVE-2019-1047 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
microsoft -- windows_7	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.	2019-06-12	4.3	CVE-2019-1048 MISC
microsoft -- windows_7	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,	2019-06-12	4.3	CVE-2019-1049 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVE-2019-1046, CVE-2019-1047, CVE-2019-1048, CVE-2019-1050.			
misp -- misp	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.	2019-06-11	6.0	CVE-2019-12794 MISC
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.14 devices. The device by default allows HTTP traffic thus providing an insecure communication mechanism for a user connecting to the web server. This allows an attacker to sniff the traffic easily and allows an	2019-06-07	4.3	CVE-2018-10690 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to compromise sensitive data such as credentials.			
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.14 devices. It is intended that an administrator can download /systemlog.log (the system log). However, the same functionality allows an attacker to download the file without any authentication or authorization.	2019-06-07	5.0	CVE-2018-10691 MISC MISC BUGTRAQ
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.14 devices. The session cookie "Password508" does not have an HttpOnly flag. This allows an attacker who is able to execute a cross-site scripting attack to steal the cookie very easily.	2019-06-07	4.3	CVE-2018-10692 MISC MISC BUGTRAQ
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.14 devices. It provides ping functionality so that an administrator can execute ICMP calls to check if the network is working correctly. However, the same functionality allows an attacker to execute commands on the device. The POST parameter "srvName" is susceptible to a buffer overflow. By crafting a packet that contains a string of 516 characters, it is possible for an attacker to execute the attack.	2019-06-07	6.8	CVE-2018-10693 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.14 devices. The device provides a Wi-Fi connection that is open and does not use any encryption mechanism by default. An administrator who uses the open wireless connection to set up the device can allow an attacker to sniff the traffic passing between the user's computer and the device. This can allow an attacker to steal the credentials passing over the HTTP connection as well as TELNET traffic. Also an attacker can MITM the response and infect a user's computer very easily as well.	2019-06-07	4.3	CVE-2018-10694 MISC MISC BUGTRAQ
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.14 devices. It provides alert functionality so that an administrator can send emails to his/her account when there are changes to the device's network. However, the same functionality allows an attacker to execute commands on the device. The POST parameters "to1,to2,to3,to4" are all susceptible to buffer overflow. By crafting a packet that contains a string of 678 characters, it is possible for an attacker to execute the attack.	2019-06-07	6.8	CVE-2018-10695 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.14 devices. The device provides a web interface to allow an administrator to manage the device. However, this interface is not protected against CSRF attacks, which allows an attacker to trick an administrator into executing actions without his/her knowledge, as demonstrated by the forms/iw_webSetParameters and forms/webSetMainRestart URIs.	2019-06-07	6.8	CVE-2018-10696 MISC MISC BUG TRAQ
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.14 devices. The Moxa AWK 3121 provides certfile upload functionality so that an administrator can upload a certificate file used for connecting to the wireless network. However, the same functionality allows an attacker to execute commands on the device. The POST parameter "iw_privatePass" is susceptible to this injection. By crafting a packet that contains shell metacharacters, it is possible for an attacker to execute the attack.	2019-06-07	6.8	CVE-2018-10699 MISC MISC BUG TRAQ
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.19 devices. It provides functionality so that an administrator can change the name of the device. However, the same functionality allows an attacker to execute XSS by injecting an XSS	2019-06-07	4.3	CVE-2018-10700 MISC MISC BUG

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	payload. The POST parameter "iw_board_deviceName" is susceptible to this injection.			TRAQ
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.14 devices. It provides functionality so that an administrator can run scripts on the device to troubleshoot any issues. However, the same functionality allows an attacker to execute commands on the device. The POST parameter "iw_filename" is susceptible to buffer overflow. By crafting a packet that contains a string of 162 characters, it is possible for an attacker to execute the attack.	2019-06-07	6.8	CVE-2018-10701 MISC MISC BUG TRAQ
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.14 devices. It provides functionality so that an administrator can run scripts on the device to troubleshoot any issues. However, the same functionality allows an attacker to execute commands on the device. The POST parameter "iw_filename" is susceptible to command injection via shell metacharacters.	2019-06-07	6.8	CVE-2018-10702 MISC MISC BUG TRAQ
moxa -- awk-3121_firmware	An issue was discovered on Moxa AWK-3121 1.14 devices. It provides functionality so that an administrator can run scripts on the	2019-06-07	6.8	CVE-2018-10703 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device to troubleshoot any issues. However, the same functionality allows an attacker to execute commands on the device. The POST parameter "iw_serverip" is susceptible to buffer overflow. By crafting a packet that contains a string of 480 characters, it is possible for an attacker to execute the attack.			MISC BUGTRAQ
omron -- network_configurator_for_devicenet_safety	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.	2019-06-12	6.8	CVE-2019-10971 MISC
panasonic -- control_fpwin_pro	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.	2019-06-07	6.8	CVE-2019-6530 BID MISC MISC MISC
panasonic -- control_fpwin_pro	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	2019-06-07	6.8	CVE-2019-6532 BID MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	expected properties. This may lead to remote code execution.			MISC MISC
phome -- empirecms	admin\db\DoSql.php in EmpireCMS through 7.5 allows remote attackers to execute arbitrary PHP code via SQL injection that uses a .php filename in a SELECT INTO OUTFILE statement to admin/admin.php.	2019-06-07	6.5	CVE-2018-19462 MISC MISC MISC MISC
photodex -- proshow_producer	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.	2019-06-10	6.8	CVE-2019-12788 MISC MISC MISC
pippo -- pippo	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.	2019-06-12	5.0	CVE-2019-5442 MISC
pix-link -- lv-wr09_firmware	XSS on the PIX-Link Repeater/Router LV-WR09 with firmware	2019-06-10	4.3	CVE-2019-11877

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	v28K.MiniRouter.20180616 allows attackers to steal credentials without being connected to the network. The attack vector is a crafted ESSID.			MISC MISC
python -- python	A security regression of CVE-2019-9636 was discovered in python since commit d537ab0ff9767ef024f2624689972 8f0116b1ec3 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 based on the application.	2019-06-07	5.0	CVE-2019-10160 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM MISC
radare -- radare2	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	2019-06-10	6.8	CVE-2019-12790 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	service (application crash) or possibly have unspecified other impact because of missing length validation in libr/egg/egg.c.			
rancher -- rancher	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.	2019-06-10	4.3	CVE-2019-11881 MISC CONFIRM
redhat -- cloudforms_management_engine	A flaw was found in the CloudForms web interface, versions 5.8 - 5.10, where the RSS feed URLs are not properly restricted to authenticated users only. An attacker could use this flaw to view potentially sensitive information from CloudForms including data such as newly created virtual machines.	2019-06-12	5.0	CVE-2017-15123 CONFIRM
redhat -- jboss_enterprise_application_platform	It was found that Picketlink as shipped with Jboss Enterprise Application Platform 7.2 would accept an xinclude parameter in	2019-06-12	6.0	CVE-2019-3873

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	SAMLresponse XML. An attacker could use this flaw to send a URL to achieve cross-site scripting or possibly conduct further attacks.			CONFIRM
redhat -- keycloak	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.	2019-06-12	5.8	CVE-2019-3875 BID CONFIRM
redhat -- openshift_container_platform	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 authentication during builds. An attacker, with the ability to redirect network traffic, could use this to alter the resulting build output.	2019-06-12	4.3	CVE-2019-10150 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
redhat -- undertow	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)	2019-06-12	5.0	CVE-2019-3888 CONFIRM
sap -- hana_extended_application_services	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.	2019-06-12	4.0	CVE-2019-0306 MISC MISC
sap -- inventory_manager	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.	2019-06-12	4.3	CVE-2019-0314 MISC MISC
sap -- netweaver_process_integration	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	2019-06-12	4.3	CVE-2019-0305 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	another application or domain, resulting in Clickjacking vulnerability. Successful exploitation of this vulnerability leads to unwanted modification of user's data.			
sap -- netweaver_process_integration	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.	2019-06-12	5.0	CVE-2019-0312 MISC MISC
sap -- netweaver_process_integration	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.	2019-06-12	5.0	CVE-2019-0315 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- r/3_enterprise	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.	2019-06-12	4.3	CVE-2019-0311 MISC MISC
securitycamera -- security_camera_cz	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.	2019-06-07	5.0	CVE-2019-12763 MISC
starry -- s00111_firmware	Starry Station (aka Starry Router) sets the Access-Control-Allow-Origin header to "*". This allows any hosted file on any domain to make calls to the device's webserver and brute force the credentials and pull any information that is stored on the device. In this case, a user's Wi-Fi credentials are stored in clear text on the device and can be pulled easily.	2019-06-10	4.3	CVE-2017-13717 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
starry -- s00111_firmware	The HTTP API supported by Starry Station (aka Starry Router) allows brute forcing the PIN setup by the user on the device, and this allows an attacker to change the Wi-Fi settings and PIN, as well as port forward and expose any internal device's port to the Internet. It was identified that the device uses custom Python code called "rodman" that allows the mobile appication to interact with the device. The APIs that are a part of this rodman Python file allow the mobile application to interact with the device using a secret, which is a uuid4 based session identifier generated by the device the first time it is set up. However, in some cases, these APIs can also use a security code. This security code is nothing but the PIN number set by the user to interact with the device when using the touch interface on the router. This allows an attacker on the Internet to interact with the router's HTTP interface when a user navigates to the attacker's website, and brute force the credentials. Also, since the device's server sets the Access-Control-Allow-Origin header to "*", an attacker can easily interact with the JSON payload returned by the device and steal sensitive information about the device.	2019-06-10	6.0	CVE-2017-13718 MISC MISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
twistedmatrix -- twisted	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.	2019-06-10	4.3	CVE-2019-12387 CONFIRM CONFIRM CONFIRM
tzumi -- klic_lock	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.	2019-06-11	4.3	CVE-2019-11334 MISC MISC
ui -- edgeos	Ubiquiti EdgeOS 1.9.1 on EdgeRouter Lite devices allows remote attackers to execute arbitrary code with admin credentials, because /opt/vyatta/share/vyatta-cfg/templates/system/static-host-mapping/host-name/node.def does not sanitize the 'alias' or 'ips' parameter for shell metacharacters.	2019-06-07	6.5	CVE-2018-5265 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ui -- unifi_firmware	Ubiquiti UniFi 52 devices, when Hotspot mode is used, allow remote attackers to bypass intended restrictions on "free time" Wi-Fi usage by sending a /guest/s/default/ request to obtain a cookie, and then using this cookie in a /guest/s/default/login request with the byfree parameter.	2019-06-07	4.3	CVE-2018-5264 MISC
urbackup -- urbackup	In UrBackup 2.2.6, an attacker can send a malformed request to the client over the network, and trigger a fileservplugin/CClientThread.cpp CClientThread::GetFileHashAndMetadata NULL pointer dereference, leading to shutting down the client application.	2019-06-07	5.0	CVE-2018-20014 MISC MISC
videolan -- vlc_media_player	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.	2019-06-13	4.3	CVE-2019-5439 MISC
wampserver -- wampserver	WampServer before 3.1.9 has CSRF in add_vhost.php because the synchronizer pattern implemented as remediation of CVE-2018-8817 was incomplete. An attacker could add/delete any vhosts without the consent of the owner.	2019-06-10	5.8	CVE-2019-11517 BUG TRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wpgraphql -- wpgraphql	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.	2019-06-10	6.4	CVE-2019-9880 MISC MISC CONFIRM MISC MISC
wpgraphql -- wpgraphql	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.	2019-06-10	5.0	CVE-2019-9881 MISC MISC CONFIRM MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
canonical -- ubuntu_linux	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	2019-06-11	3.6	CVE-2019-12749 MLIST BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(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.			MLIST BUGTRAQ UBUNTU UBUNTU DEBIAN
ibm -- intelligent_operations_center	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	2019-06-07	3.5	CVE-2019-4070 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157015.			
intel -- open_cloud_integrity_technology	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access.	2019-06-13	3.6	CVE-2019-0175 MISC
intel -- open_cloud_integrity_technology	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access.	2019-06-13	3.6	CVE-2019-0177 MISC
intel -- open_cloud_integrity_technology	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access.	2019-06-13	3.3	CVE-2019-0178 MISC
intel -- open_cloud_integrity_technology	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable	2019-06-13	3.6	CVE-2019-0179 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	information disclosure via local access.			
intel -- open_cloud_integrity_technology	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access.	2019-06-13	3.6	CVE-2019-0180 MISC
intel -- open_cloud_integrity_technology	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access.	2019-06-13	2.1	CVE-2019-0182 MISC
intel -- open_cloud_integrity_technology	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access.	2019-06-13	2.1	CVE-2019-0183 MISC
intel -- open_cloud_integrity_technology	Insufficient password protection in the attestation database for Open CIT may allow an authenticated user to potentially enable information disclosure via local access.	2019-06-13	3.6	CVE-2019-11092 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- electricflow	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.	2019-06-11	3.5	CVE-2019-10335 MLIST BID MISC
libreswan -- libreswan	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.	2019-06-12	3.5	CVE-2019-10155 CONFIRM MISC FEDORA
microsoft -- project_server	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.	2019-06-12	3.5	CVE-2019-1031 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- project_server	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.	2019-06-12	3.5	CVE-2019-1033 MISC
microsoft -- project_server	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.	2019-06-12	3.5	CVE-2019-1036 MISC
microsoft -- sharepoint_enterprise_server	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	2019-06-12	3.5	CVE-2019-1032 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVE-2019-1031, CVE-2019-1033, CVE-2019-1036.			
microsoft -- windows_10	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'.	2019-06-12	3.6	CVE-2019-0986 MISC
microsoft -- windows_10	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'.	2019-06-12	2.1	CVE-2019-1039 MISC
phome -- empirecms	admin\db\DoSql.php in EmpireCMS through 7.5 allows XSS via crafted SQL syntax to admin/admin.php.	2019-06-07	3.5	CVE-2018-19461 MISC MISC MISC
redhat -- jboss_enterprise_application_platform	It was found that a SAMLRequest containing a script could be processed by	2019-06-12	3.5	CVE-2019-3872

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			BID CONFIRM
redhat -- keycloak	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.	2019-06-12	2.1	CVE-2019-10157 BID CONFIRM
sap -- e-commerce	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.	2019-06-12	3.5	CVE-2019-0308 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- solution_manager	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.	2019-06-12	2.7	CVE-2019-0307 MISC MISC
supra -- stv-lc40lt0020f_firmware	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.	2019-06-07	2.1	CVE-2019-12477 MISC MISC
zte -- netnumen_dap_firmware	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.	2019-06-11	3.5	CVE-2019-3413 CONFIRM

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- sourcetree_for_windows	An argument injection vulnerability in Atlassian Sourcetree for Windows's URI handlers, in all versions prior to 3.1.3, allows remote attackers to gain remote code execution through the use of a crafted URI.	2019-06-14	not yet calculated	CVE-2019-11582 MISC
becton_dickinson_and_company -- alaris_gateway_workstation	BD Alaris Gateway versions, 1.0.13,1.1.3 Build 10,1.1.3 MR Build 11,1.1.5, and 1.1.6, The web browser user interface on the Alaris Gateway Workstation does not prevent an attacker with knowledge of the IP address of the Alaris Gateway Workstation terminal to gain access to the status and configuration information of the device.	2019-06-13	not yet calculated	CVE-2019-10962 BID MISC
becton_dickinson_and_company -- alaris_gateway_workstation	BD Alaris Gateway Workstation Versions, 1.1.3 Build 10, 1.1.3 MR Build 11, 1.2	2019-06-13	not yet calculated	CVE-2019-10959

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Build 15, 1.3.0 Build 14, 1.3.1 Build 13, This does not impact the latest firmware Versions 1.3.2 and 1.6.1, Additionally, the following products using software Version 2.3.6 and below, Alaris GS, Alaris GH, Alaris CC, Alaris TIVA, The application does not restrict the upload of malicious files during a firmware update.			BID MISC
belkin -- belkin_wemo_enabled_crock-pot	The Belkin Wemo Enabled Crock-Pot allows command injection in the Wemo UPnP API via the SmartDevURL argument to the SetSmartDevInfo action. A simple POST request to /upnp/control/basicevent1 can allow an attacker to execute commands without authentication.	2019-06-10	not yet calculated	CVE-2019-12780 MISC
cfme-gemset -- cfme-gemset	cfme-gemset versions 5.10.4.3 and below, 5.9.9.3 and below are vulnerable to a data leak, due to an	2019-06-14	not yet calculated	CVE-2019-10159 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	improper authorization in the migration log controller. An attacker with access to an unprivileged user can access all VM migration logs available.			
digital_persona -- u.are.u_4500_fingerprint_reader	An issue was discovered in Digital Persona U.are.U 4500 Fingerprint Reader v24. The key and salt used for obfuscating the fingerprint image exhibit cleartext when the fingerprint scanner device transfers a fingerprint image to the driver. An attacker who sniffs an encrypted fingerprint image can easily decrypt that image using the key and salt.	2019-06-13	not yet calculated	CVE-2019-12813 MISC MISC MISC
eclipse -- buildship	In Eclipse Buildship versions prior to 3.1.1, the build files indicate that this project is resolving dependencies over HTTP instead of HTTPS. Any of these artifacts could have been MITM to maliciously	2019-06-14	not yet calculated	CVE-2019-11770 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	compromise them and infect the build artifacts that were produced. Additionally, if any of these JARs or other dependencies were compromised, any developers using these could continue to be infected past updating to fix this.			
electronic_arts -- origin	An issue was discovered in Electronic Arts Origin before 10.5.39. Due to improper sanitization of the origin:// and origin2:// URI schemes, it is possible to inject additional arguments into the Origin process and ultimately leverage code execution by loading a backdoored Qt plugin remotely via the platformpluginpath argument supplied with a Windows network share.	2019-06-14	not yet calculated	CVE-2019-12828 MISC MISC MISC
embedthis -- goahead	In http.c in Embedthis GoAhead before 4.1.1 and 5.x before 5.0.1, a header parsing vulnerability causes a	2019-06-14	not yet calculated	CVE-2019-12822 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	memory assertion, out-of-bounds memory reference, and potential DoS, as demonstrated by a colon on a line by itself.			
facebook -- whatsapp	An out-of-bounds read was possible in WhatsApp due to incorrect parsing of RTP extension headers. This issue affects WhatsApp for Android prior to 2.18.276, WhatsApp Business for Android prior to 2.18.99, WhatsApp for iOS prior to 2.18.100.6, WhatsApp Business for iOS prior to 2.18.100.2, and WhatsApp for Windows Phone prior to 2.18.224.	2019-06-14	not yet calculated	CVE-2018-6350 MISC
facebook -- whatsapp	When receiving calls using WhatsApp for Android, a missing size check when parsing a sender-provided packet allowed for a stack-based overflow. This issue affects WhatsApp for Android	2019-06-14	not yet calculated	CVE-2018-6349 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	prior to 2.18.248 and WhatsApp Business for Android prior to 2.18.132.			
facebook -- whatsapp	When receiving calls using WhatsApp on Android, a stack allocation failed to properly account for the amount of data being passed in. An off-by-one error meant that data was written beyond the allocated space on the stack. This issue affects WhatsApp for Android starting in version 2.18.180 and was fixed in version 2.18.295. It also affects WhatsApp Business for Android starting in version v2.18.103 and was fixed in version v2.18.150.	2019-06-14	not yet calculated	CVE-2018-6339 MISC
facebook -- whatsapp	When receiving calls using WhatsApp for iOS, a missing size check when parsing a sender-provided packet allowed for a stack-based overflow. This issue affects WhatsApp for iOS	2019-06-14	not yet calculated	CVE-2018-20655 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	prior to v2.18.90.24 and WhatsApp Business for iOS prior to v2.18.90.24.			
gemalto -- admin_control_center	Gemalto Admin Control Center, all versions prior to 7.92, uses cleartext HTTP to communicate with www3.safenet-inc.com to obtain language packs. This allows attacker to do man-in-the-middle (MITM) attack and replace original language pack by malicious one.	2019-06-07	not yet calculated	CVE-2019-8282 MISC
gemalto -- admin_control_center	Hasplm cookie in Gemalto Admin Control Center, all versions prior to 7.92, does not have 'HttpOnly' flag. This allows malicious javascript to steal it.	2019-06-07	not yet calculated	CVE-2019-8283 MISC
huawei -- hedex_products	There is a reflection XSS vulnerability in the HedEx products. Remote attackers send malicious links to users and trick users to click. Successfully exploit cloud allow the attacker to initiate	2019-06-13	not yet calculated	CVE-2019-5286 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	XSS attacks. Affects HedEx Lite versions earlier than V200R006C00SPC007.			
ibm -- connections	IBM Connections 6.0 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: 162264.	2019-06-14	not yet calculated	CVE-2019-4403 XF CONFIRM
ibm -- i_clustering	IBM i 7.27.3 Clustering could allow a local attacker to obtain sensitive information, caused by the use of advanced node failure detection using the REST API to interface with the HMC. An attacker could exploit this vulnerability to obtain HMC credentials. IBM X-Force ID: 162159.	2019-06-14	not yet calculated	CVE-2019-4381 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- mq_advanced_cloud_pak	IBM MQ Advanced Cloud Pak (IBM Cloud Private 1.0.0 through 3.0.1) stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 159465.	2019-06-14	not yet calculated	CVE-2019-4239 XF CONFIRM
inateck -- wp1001_wireless_presenter	Due to unencrypted and unauthenticated data communication, the wireless presenter Inateck WP1001 v1.3C 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.	2019-06-07	not yet calculated	CVE-2019-12505 MISC FULLDISC BUGTRAQ MISC
inateck -- wp2002_wireless_presenter	Due to unencrypted and unauthenticated data communication, the wireless presenter Inateck WP2002 is	2019-06-07	not yet calculated	CVE-2019-12504 MISC FULL

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			DISC BUG TRAQ MISC
intel -- chipset_device_software	Improper permissions in the installer for Intel(R) Chipset Device Software (INF Update Utility) before version 10.1.1.45 may allow an authenticated user to escalate privilege via local access.	2019-06-13	not yet calculated	CVE-2019-0128 MISC
intel -- ite_tech_consumer_infrared_driver_for_windows_10	Improper permissions in the installer for the ITE Tech* Consumer Infrared Driver for Windows 10 versions before 5.4.3.0 may allow an authenticated user to potentially enable escalation of	2019-06-13	not yet calculated	CVE-2018-3702 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privilege via local access.			
intel -- multiple_microprocessors	Logic condition in specific microprocessors may allow an authenticated user to potentially enable partial physical address information disclosure via local access.	2019-06-13	not yet calculated	CVE-2019-0174 MISC
intel -- multiple_products	Insufficient input validation in HECI subsystem in Intel(R) CSME before version 11.21.55, Intel? Server Platform Services before version 4.0 and Intel? Trusted Execution Engine Firmware before version 3.1.55 may allow a privileged user to potentially enable escalation of privileges via local access.	2019-06-13	not yet calculated	CVE-2018-12147 MISC
intel -- nuc_kit	Pointer corruption in system firmware for Intel(R) NUC Kit may allow a privileged user to potentially enable escalation of privilege, denial of service and/or information	2019-06-13	not yet calculated	CVE-2019-11126 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disclosure via local access.			
intel -- nuc_kit	Buffer overflow in system firmware for Intel(R) NUC Kit may allow a privileged user to potentially enable escalation of privilege, denial of service and/or information disclosure via local access.	2019-06-13	not yet calculated	CVE-2019-11127 MISC
intel -- nuc_kit	Out of bound read/write in system firmware for Intel(R) NUC Kit may allow a privileged user to potentially enable escalation of privilege, denial of service and/or information disclosure via local access.	2019-06-13	not yet calculated	CVE-2019-11129 MISC
intel -- nuc_kit	Insufficient input validation in system firmware for Intel(R) NUC Kit may allow a privileged user to potentially enable escalation of privilege, denial of service and/or information disclosure via local access.	2019-06-13	not yet calculated	CVE-2019-11125 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
intel -- nuc_kit	Out of bound read/write in system firmware for Intel(R) NUC Kit may allow a privileged user to potentially enable escalation of privilege, denial of service and/or information disclosure via local access.	2019-06-13	not yet calculated	CVE-2019-11124 MISC
intel -- nuc_kit	Insufficient input validation in system firmware for Intel(R) NUC Kit may allow a privileged user to potentially enable escalation of privilege, denial of service and/or information disclosure via local access.	2019-06-13	not yet calculated	CVE-2019-11128 MISC
intel -- nuc_kit	Insufficient session validation in system firmware for Intel(R) NUC Kit may allow a privileged user to potentially enable escalation of privilege, denial of service and/or information disclosure via local access.	2019-06-13	not yet calculated	CVE-2019-11123 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
intel -- omni-path_fabric_manager_gui	Improper permissions in the installer for Intel(R) Omni-Path Fabric Manager GUI before version 10.9.2.1.1 may allow an authenticated user to potentially enable escalation of privilege via local attack.	2019-06-13	not yet calculated	CVE-2019-11117 MISC
intel -- proset/wireless_wifi_software_driver	Insufficient access control in the Intel(R) PROSet/Wireless WiFi Software driver before version 21.10 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2019-06-13	not yet calculated	CVE-2019-0136 MISC
intel -- raid_web_console_3	Insufficient session validation in the service API for Intel(R) RWC3 version 4.186 and before may allow an unauthenticated user to potentially enable escalation of privilege via network access.	2019-06-13	not yet calculated	CVE-2019-11119 MISC
intel -- rapid_storage_technology_enterprise	Reflected XSS in web interface for Intel(R) Accelerated Storage Manager in Intel(R)	2019-06-13	not yet calculated	CVE-2019-0130

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	RSTe before version 5.5.0.2015 may allow an unauthenticated user to potentially enable denial of service via network access.			MISC MISC
intel -- software_guard_extensions_driver_for_linux	Insufficient input validation in the Intel(R) SGX driver for Linux may allow an authenticated user to potentially enable a denial of service via local access.	2019-06-13	not yet calculated	CVE-2019-0157 MISC
leanify -- leanify	formats/xml.cpp in Leanify 0.4.3 allows for a controlled out-of-bounds write in xml_memory_writer:: write via characters that require escaping.	2019-06-15	not yet calculated	CVE-2019-12835 MISC
linksys -- wag54g2_router	On Linksys WAG54G2 1.00.10 devices, there is authenticated command injection via shell metacharacters in the setup.cgi c4_ping_ipaddr variable.	2019-06-11	not yet calculated	CVE-2009-5157 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	An issue was discovered in the Linux kernel before 4.20.15. The nfc_llcp_build_tlv function in net/nfc/llcp_commands.c may return NULL. If the caller does not check for this, it will trigger a NULL pointer dereference. This will cause denial of service. This affects nfc_llcp_build_gb in net/nfc/llcp_core.c.	2019-06-13	not yet calculated	CVE-2019-12818 MISC MISC MISC
linux -- linux_kernel	A flaw was found in the Linux kernel. A heap based buffer overflow in mwifiex_uap_parse_tail_ies function in drivers/net/wireless/marvell/mwifiex/ie.c might lead to memory corruption and possibly other consequences.	2019-06-14	not yet calculated	CVE-2019-10126 CONFIRM
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0. The function __mdiobus_register() in drivers/net/phy/mdio_bus.c calls	2019-06-13	not yet calculated	CVE-2019-12819 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	put_device(), which will trigger a fixed_mdio_bus_init use-after-free. This will cause a denial of service.			
miniblog -- miniblog	madskristensen MiniBlog through 2018-05-18 allows remote attackers to execute arbitrary ASPX code via an IMG element with a data: URL, because SaveFilesToDisk in app_code/handlers/PostHandler.cs writes a decoded base64 string to a file without validating the extension.	2019-06-14	not yet calculated	CVE-2019-9842 MISC MISC
mybb -- mybb	In MyBB before 1.8.21, an attacker can exploit a parsing flaw in the Private Message / Post renderer that leads to [video] BBCode persistent XSS to take over any forum account, aka a nested video MyCode issue.	2019-06-15	not yet calculated	CVE-2019-12830 MISC MISC
mybb -- mybb	In MyBB before 1.8.21, an attacker can	2019-06-15	not yet	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	abuse a default behavior of MySQL on many systems (that leads to truncation of strings that are too long for a database column) to create a PHP shell in the cache directory of a targeted forum via a crafted XML import, as demonstrated by truncation of aaaaaaaaaaaaaaaaaaaaaaaaaa.php.css to aaaaaaaaaaaaaaaaaaaaaaaaaa.php with a 30-character limit, aka theme import stylesheet name RCE.		calculated	12831 MISC MISC
netgear -- readynas_surveillance	In NETGEAR ReadyNAS Surveillance before 1.4.3-17 x86 and before 1.1.4-7 ARM, $_GET['uploaddir'] is not escaped and is passed to system() through $tmp_upload_dir, leading to upgrade_handle.php?cmd=writeuploaddir remote command execution.	2019-06-11	not yet calculated	CVE-2017-18378 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
orangehrm -- orangehrm	In OrangeHRM 4.3.1 and before, there is an input validation error within admin/listMailConfiguration (txtSendmailPath parameter) that allows authenticated attackers to achieve arbitrary command execution.	2019-06-15	not yet calculated	CVE-2019-12839 MISC MISC
pivotal -- spring_security_oauth	Spring Security OAuth versions 2.3 prior to 2.3.6, 2.2 prior to 2.2.5, 2.1 prior to 2.1.5, and 2.0 prior to 2.0.18, as well as older unsupported versions could be susceptible to an open redirector attack that can leak an authorization code. A malicious user or attacker can craft a request to the authorization endpoint using the authorization code grant type, and specify a manipulated redirection URI via the redirect_uri parameter. This can cause the authorization server to redirect the resource owner user-agent to a URI under the control of the attacker with the	2019-06-12	not yet calculated	CVE-2019-11269 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	leaked authorization code.			
polycom -- realpresence_debut	An issue was discovered in versions earlier than 1.3.0-66872 for Polycom RealPresence Debut that allows attackers to arbitrarily read the admin user's password via the admin web UI.	2019-06-13	not yet calculated	CVE-2018-10946 CONFIRM MISC
polycom -- realpresence_debut	An issue was discovered in versions earlier than 1.3.2 for Polycom RealPresence Debut where the admin cookie is reset only after a Debut is rebooted.	2019-06-13	not yet calculated	CVE-2018-10947 CONFIRM MISC
qualcomm -- multiple_products	Due to missing permissions in Android Manifest file, Sensitive information disclosure issue can happen in PCI RCS app in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	2019-06-14	not yet calculated	CVE-2018-13901 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS605, SD 210/SD 212/SD 205, SD 615/16/SD 415, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660			
qualcomm -- multiple_products	Out-of-Bounds write due to incorrect array index check in PMIC in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, QCS405, QCS605, Qualcomm	2019-06-14	not yet calculated	CVE-2018-13898 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130			
qualcomm -- multiple_products	Out of bounds memory read and access due to improper array index validation may lead to unexpected behavior while decoding XTRA file in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615,	2019-06-14	not yet calculated	CVE-2018-13902 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130			
qualcomm -- multiple_products	Use-after-free vulnerability will occur if reset of the routing table encounters an invalid rule id while processing command to reset in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	2019-06-14	not yet calculated	CVE-2018-13919 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, QCS405, QCS605, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24			
qualcomm -- multiple_products	While deserializing any key blob during key operations, buffer overflow could occur, exposing partial key information if any key operations are invoked in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	2019-06-14	not yet calculated	CVE-2018-13907 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCA8081, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130			
qualcomm -- multiple_products	Truncated access authentication token leads to weakened access control for stored secure	2019-06-14	not yet calculated	CVE-2018-13908 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	application data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCA8081, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/ SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130			
qualcomm -- multiple_products	Metadata verification and partial hash system calls by bootloader may corrupt parallel hashing state in progress resulting in unexpected behavior in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660,	2019-06-14	not yet calculated	CVE-2018-13909 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Snapdragon_High_Med_2016, SXR1130			
qualcomm -- multiple_products	Out-of-Bounds access in TZ due to invalid index calculated to check against DDR in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 650/52, SD 820, SD 820A, SDM439, Snapdragon_High_Med_2016	2019-06-14	not yet calculated	CVE-2018-13910 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- multiple_products	Out of bounds memory read and access may lead to unexpected behavior in GNSS XTRA Parser in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630,	2019-06-14	not yet calculated	CVE-2018-13911 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130			
qualcomm -- multiple_products	A buffer overflow can occur while processing an extscan hotlist event in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9379, QCS605, SD 625, SD 636, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20	2019-06-14	not yet calculated	CVE-2018-3583 CONFIRM
qualcomm -- multiple_products	Buffer overflow in WLAN driver event handlers due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	2019-06-14	not yet calculated	CVE-2018-5883 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Snapdragon Mobile, Snapdragon Voice & Music in MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCS405, QCS605, SD 636, SD 675, SD 730, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24			
qualcomm -- multiple_products	The HMAC authenticating the message from QSEE is vulnerable to timing side channel analysis leading to potentially forged application message in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	2019-06-14	not yet calculated	CVE-2018-13906 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Infrastructure and Networking in IPQ4019, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCA8081, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130			
qualcomm -- multiple_products	Buffer overflow in WLAN function due to improper check of buffer size before copying in Snapdragon Auto, Snapdragon	2019-06-14	not yet calculated	CVE-2018-5911 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCS605, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 855, SDM630, SDM660, SDX20, SDX24			
qualcomm -- multiple_products	Use after issue in WLAN function due to multiple ACS scan requests at a time in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCA6574AU, SD 210/SD 212/SD 205, SD 615/16/SD 415, SD 625, SD 650/52, SD 820, SDX20	2019-06-14	not yet calculated	CVE-2018-11939 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- multiple_products	Lack of input validation in WLAN function can lead to potential heap overflow in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24	2019-06-14	not yet calculated	CVE-2018-11929 CONFIRM
qualcomm -- multiple_products	Failure to initialize the reserved memory which is sent to the firmware might lead to exposure of 1 byte of uninitialized kernel SKB memory to FW in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon	2019-06-14	not yet calculated	CVE-2018-11942 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24			
qualcomm -- multiple_products	Out of bounds read occurs due to improper validation of array while processing VDEV stop response from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	2019-06-14	not yet calculated	CVE-2018-5903 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Music in MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24			
qualcomm -- multiple_products	The txrx stats req might be double freed in the pdev detach when the host driver is unloading in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8064, MDM9150, MDM9206, MDM9607, MDM9640,	2019-06-14	not yet calculated	CVE-2018-11947 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24			
qualcomm -- multiple_products	A non-time constant function memcmp is used which creates a side channel that could leak information in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	2019-06-14	not yet calculated	CVE-2018-5913 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130			
qualcomm -- multiple_products	Possible out of bounds write due to improper input validation while processing DO_ACS vendor command in Snapdragon Auto,	2019-06-14	not yet calculated	CVE-2018-11934 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24			
qualcomm -- multiple_products	Lack of check on length of reason-code fetched from payload may lead driver access the memory not allocated to the frame and results in out of bound read in Snapdragon Auto, Snapdragon Consumer	2019-06-14	not yet calculated	CVE-2018-11955 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX20, SDX24			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- multiple_products	An unprivileged user can craft a bitstream such that the payload encoded in the bitstream gains code execution in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130	2019-06-14	not yet calculated	CVE-2019-2255 CONFIRM
qualcomm -- multiple_products	An unprivileged user can craft a bitstream	2019-06-14	not yet	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	such that the payload encoded in the bitstream gains code execution in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130		calculated	2256 CONFIRM
qualcomm -- multiple_products	Wrong permissions in configuration file can lead to unauthorized	2019-06-14	not yet	CVE-2019-2257

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	permission in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 615/16/SD 415, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 855, SDA660, SDM660, SDX20, SDX24		calculated	CONFIRM
qualcomm -- multiple_products	Resource allocation error while playing the video whose dimensions are more than supported dimension in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	2019-06-14	not yet calculated	CVE-2019-2259 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130			
qualcomm -- multiple_products	Use after issue in WLAN function due to multiple ACS scan requests at a time in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU,	2019-06-14	not yet calculated	CVE-2018-11819 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 675, SD 730, SD 820A, SD 835, SD 855, SDA660, SDX20, SDX24			
qualcomm -- multiple_products	Kernel can inject faults in computations during the execution of TrustZone leading to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9615, MDM9635M,	2019-06-14	not yet calculated	CVE-2017-8252 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, SM7150, Snapdragon_High_Med_2016, SXR1130			
radare -- radare2	In radare2 through 3.5.1, the rcc_context function of libr/egg/egg_lang.c mishandles changing context. This allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact (invalid	2019-06-13	not yet calculated	CVE-2019-12802 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	memory access in r_egg_lang_parsechar; invalid free in rcc_pusharg).			
radare -- radare2	radare2 through 3.5.1 mishandles the RParse API, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact, as demonstrated by newstr buffer overflows during replace operations. This affects libr/asm/asm.c and libr/parse/parse.c.	2019-06-15	not yet calculated	CVE-2019-12829 MISC
realobjects -- pdfreactor	XXE in the XML parser library in RealObjects PDFreactor before 10.1.10722 allows attackers to supply malicious XML content in externally referenced resources, leading to disclosure of local file contents and/or denial of service conditions.	2019-06-11	not yet calculated	CVE-2019-12154 MISC CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
realobjects -- pdfreactor	Lack of validation in the HTML parser in RealObjects PDFreactor before 10.1.10722 leads to SSRF, allowing attackers to access network or file resources on behalf of the server by supplying malicious HTML content.	2019-06-11	not yet calculated	CVE-2019-12153 MISC CONFIRM CONFIRM
samsung -- galaxy_apps	Samsung Galaxy Apps before 4.4.01.7 allows modification of the hostname used for load balancing on installations of applications through a man-in-the-middle attack. An attacker may trick Galaxy Apps into using an arbitrary hostname for which the attacker can provide a valid SSL certificate, and emulate the API of the app store to modify existing apps at installation time. The specific flaw involves an HTTP method to obtain the load-balanced hostname that enforces SSL only after obtaining a	2019-06-07	not yet calculated	CVE-2018-20135 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	hostname from the load balancer, and a missing app signature validation in the application XML. An attacker can exploit this vulnerability to achieve Remote Code Execution on the device. The Samsung ID is SVE-2018-12071.			
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (Administration Console), versions 4.2, 4.3, module BILogon/appService.jsp is reflecting requested parameter errMsg into response content without sanitation. This could be used by an attacker to build a special url that execute custom JavaScript code when the url is accessed.	2019-06-14	not yet calculated	CVE-2019-0303 MISC MISC
sap -- netweaver_process_integration	SAP NetWeaver Process Integration, versions: SAP_XIESR: 7.20, SAP_XITOOL: 7.10 to 7.11, 7.30, 7.31, 7.40, 7.50, does not	2019-06-14	not yet calculated	CVE-2019-0316 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sufficiently validate user-controlled inputs, which allows an attacker possessing admin privileges to read and modify data from the victim?s browser, by injecting malicious scripts in certain servlets, which will be executed when the victim is tricked to click on those malicious links, resulting in reflected Cross Site Scripting vulnerability.			
shopware -- shopware	In createInstanceFromNamedArguments in Shopware through 5.6.x, a crafted web request can trigger a PHP object instantiation vulnerability, which can result in an arbitrary deserialization if the right class is instantiated. An attacker can leverage this deserialization to achieve remote code execution. NOTE: this issue is a bypass for a	2019-06-13	not yet calculated	CVE-2019-12799 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVE-2017-18357 whitelist patch.			
siemens -- logo!8_device	A vulnerability has been identified in SIEMENS LOGO!8 (6ED1052-xyyxx-0BA8 FS:01 to FS:06 / Firmware version V1.80.xx and V1.81.xx), SIEMENS LOGO!8 (6ED1052-xyy08-0BA0 FS:01 / Firmware version < V1.82.02). The integrated webserver does not invalidate the Session ID upon user logout. An attacker that successfully extracted a valid Session ID is able to use it even after the user logs out. The security vulnerability could be exploited by an attacker in a privileged network position who is able to read the communication between the affected device and the user or by an attacker who is able to obtain valid Session IDs through other means. The user must invoke a session	2019-06-12	not yet calculated	CVE-2019-6584 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to the affected device. At the time of advisory publication no public exploitation of this security vulnerability was known.			
siemens -- logo!8_device	A vulnerability has been identified in SIEMENS LOGO!8 (6ED1052-xyyxx-0BA8 FS:01 to FS:06 / Firmware version V1.80.xx and V1.81.xx), SIEMENS LOGO!8 (6ED1052-xyy08-0BA0 FS:01 / Firmware version < V1.82.02). An attacker with network access to port 10005/tcp of the LOGO! device could cause a Denial-of-Service condition by sending specially crafted packets. The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected service. No user interaction is required to exploit this security vulnerability. Successful exploitation of the security vulnerability	2019-06-12	not yet calculated	CVE-2019-6571 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	compromises availability of the targeted system. At the time of advisory publication no public exploitation of this security vulnerability was known.			
siemens -- multiple_scalance_products	A vulnerability has been identified in SCALANCE X-200 (All Versions < V5.2.4), SCALANCE X-200IRT (All versions), SCALANCE X-300 (All versions), SCALANCE X-414-3E (All versions). The affected devices store passwords in a recoverable format. An attacker may extract and recover device passwords from the device configuration. Successful exploitation requires access to a device configuration backup and impacts confidentiality of the stored passwords. At the time of advisory publication no public exploitation of this	2019-06-12	not yet calculated	CVE-2019-6567 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	security vulnerability was known.			
siemens -- simatic_ident_mv420_and_mv440_families	A vulnerability has been identified in SIMATIC Ident MV420 family (All versions), SIMATIC Ident MV440 family (All versions). Communication with the device is not encrypted. Data transmitted between the device and the user can be obtained by an attacker in a privileged network position. The security vulnerability can be exploited by an attacker in a privileged network position which allows evesdropping the communication between the affected device and the user. The user must invoke a session. Successful exploitation of the vulnerability compromises confidentiality of the data transmitted. At the time of advisory publication no public exploitation of this	2019-06-12	not yet calculated	CVE-2019-10926 BID MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	security vulnerability was known.			
siemens -- simatic_ident_mv420_and_mv440_families	A vulnerability has been identified in SIMATIC Ident MV420 family (All versions), SIMATIC Ident MV440 family (All versions). An authenticated attacker could escalate privileges by sending specially crafted requests to the integrated webserver. The security vulnerability can be exploited by an attacker with network access to the device. Valid user credentials, but no user interaction are required. Successful exploitation compromises integrity and availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known.	2019-06-12	not yet calculated	CVE-2019-10925 BID MISC MISC
siemens -- siveillance_vms	A vulnerability has been identified in Siveillance VMS 2017	2019-06-12	not yet	CVE-2019-6582

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	R2 (All versions < V11.2a), Siveillance VMS 2018 R1 (All versions < V12.1a), Siveillance VMS 2018 R2 (All versions < V12.2a), Siveillance VMS 2018 R3 (All versions < V12.3a), Siveillance VMS 2019 R1 (All versions < V13.1a). An attacker with network access to port 80/TCP can change user-defined event properties without proper authorization. The security vulnerability could be exploited by an authenticated attacker with network access to the affected service. No user interaction is required to exploit this security vulnerability. Successful exploitation compromises integrity of the user-defined event properties and the availability of corresponding functionality. At the time of advisory publication no public exploitation of this		calculated	MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	security vulnerability was known.			
siemens -- siveillance_vms	A vulnerability has been identified in Siveillance VMS 2017 R2 (All versions < V11.2a), Siveillance VMS 2018 R1 (All versions < V12.1a), Siveillance VMS 2018 R2 (All versions < V12.2a), Siveillance VMS 2018 R3 (All versions < V12.3a), Siveillance VMS 2019 R1 (All versions < V13.1a). An attacker with network access to port 80/TCP could change user roles without proper authorization. The security vulnerability could be exploited by an authenticated attacker with network access to the affected service. No user interaction is required to exploit this security vulnerability. Successful exploitation compromises confidentiality, integrity and availability of the	2019-06-12	not yet calculated	CVE-2019-6581 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	targeted system. At the time of advisory publication no public exploitation of this security vulnerability was known.			
siemens -- siveillance_vms	A vulnerability has been identified in Siveillance VMS 2017 R2 (All versions < V11.2a), Siveillance VMS 2018 R1 (All versions < V12.1a), Siveillance VMS 2018 R2 (All versions < V12.2a), Siveillance VMS 2018 R3 (All versions < V12.3a), Siveillance VMS 2019 R1 (All versions < V13.1a). An attacker with network access to port 80/TCP could change device properties without authorization. No user interaction is required to exploit this security vulnerability. Successful exploitation compromises confidentiality, integrity and availability of the targeted system. At the time of advisory	2019-06-12	not yet calculated	CVE-2019-6580 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	publication no public exploitation of this security vulnerability was known.			
silverstripe -- silverstripe/restfulserver_module_and_silverstripe/registry	SQL injection vulnerability in silverstripe/restfulserver module 1.0.x before 1.0.9, 2.0.x before 2.0.4, and 2.1.x before 2.1.2 and silverstripe/restfulserver module 2.1.x before 2.1.1 and 2.2.x before 2.2.1 allows attackers to execute arbitrary SQL commands.	2019-06-11	not yet calculated	CVE-2019-12149 CONFIRM
ubiquiti -- multiple_devices	On certain Ubiquiti devices, Command Injection exists via a GET request to stainfo.cgi (aka Show AP info) because the ifname variable is not sanitized, as demonstrated by shell metacharacters. The fixed version is v4.0.1 for 802.11 ISP products, v5.3.5 for AirMax ISP products, and v5.4.5 for AirSync firmware. For example, Nanostation5 (Air OS) is affected.	2019-06-11	not yet calculated	CVE-2010-5330 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
webmin -- webmin	In Webmin through 1.910, any user authorized to the "Package Updates" module can execute arbitrary commands with root privileges via the data parameter to update.cgi.	2019-06-15	not yet calculated	CVE-2019-12840 MISC MISC
wordpress -- wordpress	The "Count per Day" plugin before 3.2.6 for WordPress allows XSS via the wp-admin/?page=cpd_metaboxes daytoshow parameter.	2019-06-15	not yet calculated	CVE-2013-7472 MISC MISC
zhejiang_dahua_technology -- dahua_ip_camera_devices	Buffer overflow vulnerability found in some Dahua IP Camera devices IPC-HFW1XXX,IPC-HDW1XXX,IPC-HFW2XXX Build before 2018/11. The vulnerability exits in the function of redirection display for serial port printing information, which can not be used by product basic functions. After an attacker logs in locally, this vulnerability can be exploited to cause	2019-06-12	not yet calculated	CVE-2019-9676 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device restart or arbitrary code execution. Dahua has identified the corresponding security problems in the static code auditing process, so it has gradually deleted this function, which is no longer available in the newer devices and softwares. Dahua has released versions of the affected products to fix the vulnerability.			
znc -- znc	Modules.cpp in ZNC before 1.7.4-rc1 allows remote authenticated non-admin users to escalate privileges and execute arbitrary code by loading a module with a crafted name.	2019-06-15	not yet calculated	CVE-2019-12816 CONFIRM CONFIRM
zte -- mf920_router	All versions up to BD_R218V2.4 of ZTE MF920 product are impacted by information leak vulnerability. Due to some interfaces can obtain the WebUI login password without login, an attacker can exploit the vulnerability to	2019-06-11	not yet calculated	CVE-2019-3411 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	obtain sensitive information about the affected components.			
zte -- mf920_router	All versions up to BD_R218V2.4 of ZTE MF920 product are impacted by command execution vulnerability. Due to some interfaces do not adequately verify parameters, an attacker can execute arbitrary commands through specific interfaces.	2019-06-11	not yet calculated	CVE-2019-3412 CONFIRM
zte -- wf820+_lte_outdoor_cpe	All versions up to UKBB_WF820+_1.0.0B06 of ZTE WF820+ LTE Outdoor CPE product are impacted by command injection vulnerability. Due to inadequate parameter verification, unauthorized users can take advantage of this vulnerability to control the user terminal system.	2019-06-11	not yet calculated	CVE-2019-3409 CONFIRM
zte -- wf820+_lte_outdoor_cpe	All versions up to UKBB_WF820+_1.0.0B06 of ZTE WF820+ LTE Outdoor CPE product are impacted	2019-06-11	not yet calculated	CVE-2019-3410 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	by Cross-Site Request Forgery vulnerability,which stems from the fact that WEB applications do not adequately verify whether requests come from trusted users. An attacker can exploit this vulnerability to send unexpected requests to the server through the affected client.			