Vulnerability Summary for the Week of January 7, 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
microsoft -- edge	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge.	2019-01-08	7.6	CVE-2019-0565 BID CONFIRM

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arc_project -- arc	ARC 5.21q allows directory traversal via a full pathname in an archive file.	2019-01-07	5.0	CVE-2015-9275 MISC MISC
getbootstrap -- bootstrap	In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.	2019-01-09	4.3	CVE-2016-10735 MISC MISC MISC MISC MISC MISC
ibm -- api_connect	IBM API Connect 5.0.0.0 through 5.0.8.4 could allow a user authenticated as an administrator with	2019-01-04	6.5	CVE-2018-1859 BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	limited rights to escalate their privileges. IBM X-Force ID: 151258.			XF CONFIRM
microsoft -- asp.net_core	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka "ASP.NET Core Denial of Service Vulnerability." This affects ASP.NET Core 2.1. This CVE ID is unique from CVE-2019-0548.	2019-01-08	5.0	CVE-2019-0564 BID REDHAT CONFIRM
microsoft -- office	An information disclosure vulnerability exists when Microsoft Outlook improperly handles certain types of messages, aka "Microsoft Outlook Information Disclosure Vulnerability." This affects Office 365 ProPlus, Microsoft Office, Microsoft Outlook.	2019-01-08	4.3	CVE-2019-0559 BID CONFIRM
microsoft -- office	An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory, aka "Microsoft Office Information Disclosure Vulnerability." This affects Office 365 ProPlus, Microsoft Office.	2019-01-08	4.3	CVE-2019-0560 BID CONFIRM
yunucms -- yunucms	YUNUCMS 1.1.8 has XSS in app/admin/controller/System.php because crafted data can be written to the sys.php file, as demonstrated by site_title in an admin/system/basic POST request.	2019-01-04	4.3	CVE-2019-5310 MISC
yunucms -- yunucms	An issue was discovered in YUNUCMS V1.1.8. app/index/controller/Show.php has an XSS vulnerability via the index.php/index/show/index cw parameter.	2019-01-04	4.3	CVE-2019-5311 MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
frog_cms_project -- frog_cms	Frog CMS 0.9.5 has XSS in the admin/?/page/edit/1 body field.	2019-01-09	3.5	CVE-2018-20680 MISC
ibm -- rational_publishing_engine	IBM Publishing Engine 2.1.2, 6.0.5, and 6.0.6 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	2019-01-04	3.5	CVE-2018-1657 BID XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a trusted session. IBM X-force ID: 144883.			
ibm -- rational_publishing_engine	IBM Publishing Engine 2.1.2, 6.0.5, and 6.0.6 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: 153494.	2019-01-04	3.5	CVE-2018-1951 BID XF CONFIRM

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- karaf	Apache Karaf provides a features deployer, which allows users to "hot deploy" a features XML by dropping the file directly in the deploy folder. The features XML is parsed by XMLInputFactory class. Apache Karaf XMLInputFactory class doesn't contain any mitigation codes against XXE. This is a potential security risk as an user can inject external XML entities in Apache Karaf version prior to 4.1.7 or 4.2.2. It has been fixed in Apache Karaf 4.1.7 and 4.2.2 releases.	2019-01-07	not yet calculated	CVE-2018-11788 MISC BID
apache -- thrift	Apache Thrift Java client library versions 0.5.0 through 0.11.0 can bypass SASL negotiation isComplete validation in the org.apache.thrift.transport.TSaslTransport class. An assert used to determine if the SASL handshake had successfully completed could be disabled in production settings making the validation incomplete.	2019-01-07	not yet calculated	CVE-2018-1320 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- thrift	The Apache Thrift Node.js static web server in versions 0.9.2 through 0.11.0 have been determined to contain a security vulnerability in which a remote user has the ability to access files outside the set webservers docroot path.	2019-01-07	not yet calculated	CVE-2018-11798 BID MISC
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the Clean My Mac X, version 4.04, helper service due to improper input validation. A user with local access can use this vulnerability to modify the file system as root. An attacker would need local access to the machine for a successful exploit.	2019-01-10	not yet calculated	CVE-2018-4043 MISC
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4047 MISC
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the way the CleanMyMac X software improperly validates inputs. An attacker with local access could use this vulnerability to modify the file system as root. An attacker would need local access to the machine for a successful exploit.	2019-01-10	not yet calculated	CVE-2018-4032 MISC
apple -- cleanmymac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability due to improper input validation. An attacker with local access could use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4033 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- cleanmymac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability that exists due to improper input validation. An attacker with local access could use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4034 MISC
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4045 MISC
apple -- cleanmymac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability due to improper input validation. An attacker with local access could use this vulnerability to modify the running kernel extensions on the system.	2019-01-10	not yet calculated	CVE-2018-4036 MISC
apple -- cleanmymac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability due to improper input validation. An attacker with local access can use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4037 MISC
apple -- cleanmymac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability that exists due to improper input validation. An attacker with local access could use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4035 MISC
apple -- cleanmymac_x	An exploitable denial-of-service vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. A user with local access	2019-01-10	not yet calculated	CVE-2018-4046 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	can use this vulnerability to terminate a privileged helper application. An attacker would need local access to the machine for a successful exploit.			
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4041 MISC
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4042 MISC
apple -- cleanmymac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	CVE-2018-4044 MISC
apple -- ios	In iOS before 11.2, exchange rates were retrieved from HTTP rather than HTTPS. This was addressed by enabling HTTPS for exchange rates.	2019-01-11	not yet calculated	CVE-2017-2411 CONFIRM
apple -- ios	In iOS before 11.4 and macOS High Sierra before 10.13.5, a memory corruption issue exists and was addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4404 MISC CONFIRM EXPL

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				OIT-DB
apple -- ios	In iOS before 11.2, an inconsistent user interface issue was addressed through improved state management.	2019-01-11	not yet calculated	CVE-2017-13891 CONFIRM
apple -- ios	In iOS before 11.2, a type confusion issue was addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2017-13888 CONFIRM
apple -- ios	In iOS before 11.4, a memory corruption issue exists and was addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4330 BID SECTRACK CONFIRM
apple -- ios	In iOS before 9.3.3, a memory corruption issue existed in the kernel. This issue was addressed through improved memory handling.	2019-01-11	not yet calculated	CVE-2016-7576 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved size validation.	2019-01-11	not yet calculated	CVE-2018-4257 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	CVE-2018-4255 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an input validation issue existed in the kernel. This issue was addressed with improved input validation.	2019-01-11	not yet calculated	CVE-2018-4254 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, a privacy issue in the handling of Open Directory records was addressed with improved indexing.	2019-01-11	not yet calculated	CVE-2018-4217 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an access issue was addressed with additional sandbox restrictions.	2019-01-11	not yet calculated	CVE-2018-4183 CONFIRM DEBIAN
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an access issue was addressed with additional sandbox restrictions on CUPS.	2019-01-11	not yet calculated	CVE-2018-4182 CONFIRM DEBIAN
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.	2019-01-11	not yet calculated	CVE-2018-4181 MLIST CONFIRM UBUNTU DEBIAN
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.	2019-01-11	not yet calculated	CVE-2018-4180 MLIST CONFIRM UBUNTU DEBIAN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved bounds checking.	2019-01-11	not yet calculated	CVE-2018-4258 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	CVE-2018-4256 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.4, there was an issue with the handling of smartcard PINs. This issue was addressed with additional logic.	2019-01-11	not yet calculated	CVE-2018-4179 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.2, an access issue existed with privileged WiFi system configuration. This issue was addressed with additional restrictions.	2019-01-11	not yet calculated	CVE-2017-13886 CONFIRM
apple -- macos_high_sierra	In macOS High Sierra before 10.13.2, a logic issue existed in APFS when deleting keys during hibernation. This was addressed with improved state management.	2019-01-11	not yet calculated	CVE-2017-13887 CONFIRM
apple -- multiple_products	In iOS before 11.4, iCloud for Windows before 7.5, watchOS before 4.3.1, iTunes before 12.7.5 for Windows, and macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	CVE-2018-4194 MISC CONFIRM MISC MISC MISC
apple -- multiple_products	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, a logic error existed in the validation of credentials. This was addressed with improved credential validation.	2019-01-11	not yet calculated	CVE-2017-13889 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	CVE-2018-4169 CONFIRM
apple -- multiple_products	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, sound fetched through audio elements may be exfiltrated cross-origin. This issue was addressed with improved audio taint tracking.	2019-01-11	not yet calculated	CVE-2018-4278 SECTRACK GENTOO CONFIRM MISC MISC MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.4.1, watchOS before 4.3.2, tvOS before 11.4.1, Safari before 11.1.1, macOS High Sierra before 10.13.6, a spoofing issue existed in the handling of URLs. This issue was addressed with improved input validation.	2019-01-11	not yet calculated	CVE-2018-4277 SECTRACK MISC MISC MISC CONFIRM MISC
apple -- multiple_products	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, multiple memory corruption issues were addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4262 SECTRACK GENTOO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC CONFIRM MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4213 GENTOO MISC CONFIRM MISC MISC MISC UBUNTU
apple -- multiple_products	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, a permissions issue existed in Remote Management. This issue was addressed through improved permission validation.	2019-01-11	not yet calculated	CVE-2018-4298 CONFIRM MISC
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4212 GENTOO MISC CONFIRM MISC MISC MISC UBUNTU

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, an array indexing issue existed in the handling of a function in javascript core. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4210 GENTOO MISC MISC MISC CONFIRM UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4209 GENTOO MISC CONFIRM MISC MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4208 GENTOO MISC MISC MISC CONFIRM MISC MISC UBUNTU

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4207 GENTOO MISC CONFIRM MISC MISC MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.2.5, macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, watchOS before 4.2.2, and tvOS before 11.2.5, a memory corruption issue exists and was addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4189 CONFIRM MISC MISC MISC
apple -- multiple_products	In iCloud for Windows before 7.3, Safari before 11.0.3, iTunes before 12.7.3 for Windows, and iOS before 11.2.5, multiple memory corruption issues exist and were addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4147 CONFIRM MISC MISC MISC MISC
apple -- multiple_products	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, a downgrade issue existed with HTTP authentication credentials saved in Keychain. This issue was addressed by storing the authentication types with the credentials.	2019-01-11	not yet calculated	CVE-2016-4644 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, a validation issue existed in the parsing of 407 responses. This issue was addressed through improved response validation.	2019-01-11	not yet calculated	CVE-2016-4643 MISC MISC CONFIRM
apple -- multiple_products	In iOS before 11.3, tvOS before 11.3, watchOS before 4.3, and macOS before High Sierra 10.13.4, an information disclosure issue existed in the transition of program state. This issue was addressed with improved state handling.	2019-01-11	not yet calculated	CVE-2018-4185 MISC MISC CONFIRM MISC
apple -- multiple_products	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, proxy authentication incorrectly reported HTTP proxies received credentials securely. This issue was addressed through improved warnings.	2019-01-11	not yet calculated	CVE-2016-4642 MISC MISC CONFIRM
apple -- safari	In Safari before 11.1, an information leakage issue existed in the handling of downloads in Safari Private Browsing. This issue was addressed with additional validation.	2019-01-11	not yet calculated	CVE-2018-4186 CONFIRM
apple -- swiftnio	In SwiftNIO before 1.8.0, a buffer overflow was addressed with improved size validation.	2019-01-11	not yet calculated	CVE-2018-4281 CONFIRM
artifex -- mupdf	Artifex MuPDF 1.14.0 has a SEGV in the function fz_load_page of the fitz/document.c file, as demonstrated by mutool. This is related to page-number mishandling in cbz/mucbz.c, cbz/muimg.c, and svg/svg-doc.c.	2019-01-11	not yet calculated	CVE-2019-6130 MISC
artifex -- mupdf	svg-run.c in Artifex MuPDF 1.14.0 has infinite recursion with stack consumption in	2019-01-11	not yet	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	svg_run_use_symbol, svg_run_element, and svg_run_use, as demonstrated by mutool.		calculated	6131 MISC
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via FactoryPassword parameter or bootmode parameter of a certain URL.	2019-01-09	not yet calculated	CVE-2018-0634 MISC JVN
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via filename parameter.	2019-01-09	not yet calculated	CVE-2018-0635 MISC JVN
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via FactoryPassword parameter of a certain URL, different URL from CVE-2018-0634.	2019-01-09	not yet calculated	CVE-2018-0636 MISC JVN
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via import.cgi encKey parameter.	2019-01-09	not yet calculated	CVE-2018-0638 MISC JVN
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via tools_firmware.cgi date parameter, time parameter, and offset parameter.	2019-01-09	not yet calculated	CVE-2018-0639 MISC JVN
aterm -- hc100rc	Buffer overflow in Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary code via netWizard.cgi date parameter, time parameter, and offset parameter.	2019-01-09	not yet calculated	CVE-2018-0640 MISC JVN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aterm -- hc100rc	Buffer overflow in Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary code via tools_system.cgi date parameter, time parameter, and offset parameter.	2019-01-09	not yet calculated	CVE-2018-0641 MISC JVN
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via export.cgi encKey parameter.	2019-01-09	not yet calculated	CVE-2018-0637 MISC JVN
aterm -- w300p	Buffer overflow in Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary code via submit-url parameter.	2019-01-09	not yet calculated	CVE-2018-0633 MISC JVN
aterm -- w300p	Buffer overflow in Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary code via HTTP request and response.	2019-01-09	not yet calculated	CVE-2018-0632 MISC JVN
aterm -- w300p	Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary OS commands via targetAPSsid parameter.	2019-01-09	not yet calculated	CVE-2018-0631 MISC JVN
aterm -- w300p	Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary OS commands via HTTP request and response.	2019-01-09	not yet calculated	CVE-2018-0629 MISC JVN
aterm -- w300p	Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary OS commands via sysCmd parameter.	2019-01-09	not yet calculated	CVE-2018-0630 MISC JVN
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via HTTP request and response.	2019-01-09	not yet calculated	CVE-2018-0628 MISC JVN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via targetAPSsid parameter.	2019-01-09	not yet calculated	CVE-2018-0627 MISC JVN
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via sysCmd in formWsc parameter.	2019-01-09	not yet calculated	CVE-2018-0626 MISC JVN
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via formSysCmd parameter.	2019-01-09	not yet calculated	CVE-2018-0625 MISC JVN
bento4 -- bento4	An issue was discovered in Bento4 v1.5.1-627. There is a memory leak in AP4_DescriptorFactory::CreateDescriptorFromStream in Core/Ap4DescriptorFactory.cpp when called from the AP4_EsdsAtom class in Core/Ap4EsdsAtom.cpp, as demonstrated by mp42aac.	2019-01-11	not yet calculated	CVE-2019-6132 MISC
bodhi -- bodhi	Bodhi 2.9.0 and lower is vulnerable to cross-site scripting resulting in code injection caused by incorrect validation of bug titles.	2019-01-10	not yet calculated	CVE-2017-1002152 CONFIRM
bootstrap -- bootstrap	In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.	2019-01-09	not yet calculated	CVE-2018-20677 MISC MISC MISC MISC
bootstrap -- bootstrap	In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.	2019-01-09	not yet	CVE-2018-20676

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
			calculated	MISC MISC MISC MISC MISC
busybox -- busybox	An issue was discovered in BusyBox through 1.30.0. An out of bounds read in udhcp components (consumed by the DHCP server, client, and/or relay) might allow a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. This is related to assurance of a 4-byte length when decoding DHCP_SUBNET. NOTE: this issue exists because of an incomplete fix for CVE-2018-20679.	2019-01-09	not yet calculated	CVE-2019-5747 MISC MISC
busybox -- busybox	An issue was discovered in BusyBox before 1.30.0. An out of bounds read in udhcp components (consumed by the DHCP server, client, and relay) allows a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. This is related to verification in udhcp_get_option() in networking/udhcp/common.c that 4-byte options are indeed 4 bytes.	2019-01-09	not yet calculated	CVE-2018-20679 MISC MISC MISC
cimtechniques -- cimscan	In CIMTechniques CIMScan 6.x through 6.2, the SOAP WSDL parser allows attackers to execute SQL code.	2019-01-10	not yet calculated	CVE-2018-16803 MISC MISC
cisco -- 900_series_aggregation_services_router	A vulnerability in Cisco 900 Series Aggregation Services Router (ASR) software could allow an unauthenticated, remote attacker to cause a partial denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient handling of certain	2019-01-11	not yet calculated	CVE-2018-15464 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	broadcast packets ingress to the device. An attacker could exploit this vulnerability by sending large streams of broadcast packets to an affected device. If successful, an exploit could allow an attacker to impact services running on the device, resulting in a partial DoS condition.			
cisco -- cisco_asyncos_software_for_cisco_email_security_appliance	A vulnerability in the Secure/Multipurpose Internet Mail Extensions (S/MIME) Decryption and Verification or S/MIME Public Key Harvesting features of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to cause an affected device to corrupt system memory. A successful exploit could cause the filtering process to unexpectedly reload, resulting in a denial of service (DoS) condition on the device. The vulnerability is due to improper input validation of S/MIME-signed emails. An attacker could exploit this vulnerability by sending a malicious S/MIME-signed email through a targeted device. If Decryption and Verification or Public Key Harvesting is configured, the filtering process could crash due to memory corruption and restart, resulting in a DoS condition. The software could then resume processing the same S/MIME-signed email, causing the filtering process to crash and restart again. A successful exploit could allow the attacker to cause a permanent DoS condition. This vulnerability may	2019-01-10	not yet calculated	CVE-2018-15453 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	require manual intervention to recover the ESA.			
cisco -- cisco_asyncos_software_for_cisco_email_security_appliance	A vulnerability in the email message filtering feature of Cisco AsyncOS Software for Cisco Email Security Appliances (ESA) could allow an unauthenticated, remote attacker to cause the CPU utilization to increase to 100 percent, causing a denial of service (DoS) condition on an affected device. The vulnerability is due to improper filtering of email messages that contain references to whitelisted URLs. An attacker could exploit this vulnerability by sending a malicious email message that contains a large number of whitelisted URLs. A successful exploit could allow the attacker to cause a sustained DoS condition that could force the affected device to stop scanning and forwarding email messages.	2019-01-10	not yet calculated	CVE-2018-15460 BID CISCO
cisco -- firepower_management_center	A vulnerability in the Shell Access Filter feature of Cisco Firepower Management Center (FMC), when used in conjunction with remote authentication, could allow an unauthenticated, remote attacker to cause high disk utilization, resulting in a denial of service (DoS) condition. The vulnerability occurs because the configuration of the Shell Access Filter, when used with a specific type of remote authentication, can cause a system file to have unbounded writes. An attacker could exploit this vulnerability by sending a steady stream of remote authentication requests to the appliance when the specific configuration is applied.	2019-01-10	not yet calculated	CVE-2018-15458 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Successful exploitation could allow the attacker to increase the size of a system log file so that it consumes most of the disk space. The lack of available disk space could lead to a DoS condition in which the device functions could operate abnormally, making the device unstable.			
cisco -- identity_services_engine	A vulnerability in the Admin Portal of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to view saved passwords in plain text. The vulnerability is due to the incorrect inclusion of saved passwords when loading configuration pages in the Admin Portal. An attacker with read or write access to the Admin Portal could exploit this vulnerability by browsing to a page that contains sensitive data. An exploit could allow the attacker to recover passwords for unauthorized use and expose those accounts to further attack.	2019-01-10	not yet calculated	CVE-2018-15456 BID CISCO
cisco -- ios_and_ios_xe_software	A vulnerability in the TCP socket code of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. The vulnerability is due to a state condition between the socket state and the transmission control block (TCB) state. While this vulnerability potentially affects all TCP applications, the only affected application observed so far is the HTTP server. An attacker could exploit this vulnerability by sending specific HTTP requests at a sustained rate to a reachable IP address of the affected software. A	2019-01-09	not yet calculated	CVE-2018-0282 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition on an affected device.			
cisco -- ios_and_ios_xe_software	A vulnerability in the access control logic of the Secure Shell (SSH) server of Cisco IOS and IOS XE Software may allow connections sourced from a virtual routing and forwarding (VRF) instance despite the absence of the vrf-also keyword in the access-class configuration. The vulnerability is due to a missing check in the SSH server. An attacker could use this vulnerability to open an SSH connection to an affected Cisco IOS or IOS XE device with a source address belonging to a VRF instance. Once connected, the attacker would still need to provide valid credentials to access the device.	2019-01-10	not yet calculated	CVE-2018-0484 CISCO
cisco -- ip_phone_8800_series_software	A vulnerability in the Cisco IP Phone 8800 Series Software could allow an unauthenticated, remote attacker to conduct an arbitrary script injection attack on an affected device. The vulnerability exists because the software running on an affected device insufficiently validates user-supplied data. An attacker could exploit this vulnerability by persuading a user to click a malicious link provided to the user or through the interface of an affected device. A successful exploit could allow an attacker to execute arbitrary script code in the context of the user interface or access sensitive system-based information, which	2019-01-10	not yet calculated	CVE-2018-0461 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	under normal circumstances should be prohibited.			
cisco -- jabber_client_framework	A vulnerability in the Cisco Jabber Client Framework (JCF) software, installed as part of the Cisco Jabber for Mac client, could allow an authenticated, local attacker to corrupt arbitrary files on an affected device that has elevated privileges. The vulnerability exists due to insecure directory permissions set on a JCF created directory. An authenticated attacker with the ability to access an affected directory could create a hard link to an arbitrary location on the affected system. An attacker could convince another user that has administrative privileges to perform an install or update the Cisco Jabber for Mac client to perform such actions, allowing files to be created in an arbitrary location on the disk or an arbitrary file to be corrupted when it is appended to or overwritten.	2019-01-10	not yet calculated	CVE-2018-0449 BID CISCO
cisco -- jabber_client_framework	A vulnerability in Cisco Jabber Client Framework (JCF) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of an affected system. The vulnerability is due to insufficient validation of user-supplied input of an affected client. An attacker could exploit this vulnerability by executing arbitrary JavaScript in the Jabber client of the recipient. A successful exploit could allow the attacker to execute arbitrary script code in the context of the targeted client or allow the attacker to access sensitive client-based information.	2019-01-10	not yet calculated	CVE-2018-0483 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- policy_suite_for_mobile_and_policy_suite_diameter_routing_agent_software	A vulnerability in the Redis implementation used by the Cisco Policy Suite for Mobile and Cisco Policy Suite Diameter Routing Agent software could allow an unauthenticated, remote attacker to modify key-value pairs for short-lived events stored by the Redis server. The vulnerability is due to improper authentication when accessing the Redis server. An unauthenticated attacker could exploit this vulnerability by modifying key-value pairs stored within the Redis server database. An exploit could allow the attacker to reduce the efficiency of the Cisco Policy Suite for Mobile and Cisco Policy Suite Diameter Routing Agent software.	2019-01-09	not yet calculated	CVE-2018-0181 CISCO
cisco -- policy_suite	A vulnerability in the Graphite web interface of the Policy and Charging Rules Function (PCRF) of Cisco Policy Suite (CPS) could allow an unauthenticated, remote attacker to access the Graphite web interface. The attacker would need to have access to the internal VLAN where CPS is deployed. The vulnerability is due to lack of authentication. An attacker could exploit this vulnerability by directly connecting to the Graphite web interface. An exploit could allow the attacker to access various statistics and Key Performance Indicators (KPIs) regarding the Cisco Policy Suite environment.	2019-01-11	not yet calculated	CVE-2018-15466 BID CISCO
cisco -- prime_infrastructure	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an unauthenticated, remote attacker to	2019-01-10	not yet calculated	CVE-2018-15457 BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected system. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.			CISCO
cisco -- prime_network_control_system	A vulnerability in the web-based management interface of Cisco Prime Network Control System could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web interface of the affected system. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web-based management interface or allow the attacker to access sensitive browser-based information.	2019-01-10	not yet calculated	CVE-2018-0482 BID CISCO
cisco -- telepresence_management_suite	A vulnerability in the web-based management interface of Cisco TelePresence Management Suite (TMS) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS)	2019-01-11	not yet calculated	CVE-2018-15467 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.			
cisco -- unified_communications_manager	A vulnerability in the web-based management interface of Cisco Unified Communications Manager could allow an authenticated, remote attacker to view digest credentials in clear text. The vulnerability is due to the incorrect inclusion of saved passwords in configuration pages. An attacker could exploit this vulnerability by logging in to the Cisco Unified Communications Manager web-based management interface and viewing the source code for the configuration page. A successful exploit could allow the attacker to recover passwords and expose those accounts to further attack.	2019-01-10	not yet calculated	CVE-2018-0474 CISCO
cisco -- webex_business_suite	A vulnerability in the MyWebex component of Cisco Webex Business Suite could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by	2019-01-10	not yet calculated	CVE-2018-15461 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	convincing a user to click a crafted URL. To exploit this vulnerability, the attacker may provide a link that directs a user to a malicious site and use misleading language or instructions to persuade the user to follow the provided link.			
cybozu -- dezie	Directory traversal vulnerability in Cybozu Dezie 8.0.2 to 8.1.2 allows remote attackers to read arbitrary files via HTTP requests.	2019-01-09	not yet calculated	CVE-2018-0705 JVN MISC
cybozu -- garoon	Cybozu Garoon 3.0.0 to 4.10.0 allows remote attackers to bypass access restriction to view information available only for a sign-on user via Single sign-on function.	2019-01-09	not yet calculated	CVE-2018-16178 JVN MISC
cybozu -- mailwise	Directory traversal vulnerability in Cybozu Mailwise 5.0.0 to 5.4.5 allows remote attackers to delete arbitrary files via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-0702 JVN MISC
cybozu -- office	Directory traversal vulnerability in Cybozu Office 10.0.0 to 10.8.1 allows remote attackers to delete arbitrary files via HTTP requests.	2019-01-09	not yet calculated	CVE-2018-0703 JVN MISC
cybozu -- office	Directory traversal vulnerability in Cybozu Office 10.0.0 to 10.8.1 allows remote attackers to delete arbitrary files via Keitai Screen.	2019-01-09	not yet calculated	CVE-2018-0704 JVN MISC
cybozu -- remote_service	Cybozu Remote Service 3.0.0 to 3.1.0 allows remote authenticated attackers to upload and execute Java code file on the server via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16169 JVN MISC
cybozu -- remote_service	Improper countermeasure against clickjacking attack in client certificates management screen was discovered in Cybozu Remote	2019-01-09	not yet calculated	CVE-2018-16172

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Service 3.0.0 to 3.1.8, that allows remote attackers to trick a user to delete the registered client certificate.			JVN MISC
cybozu -- remote_service	Directory traversal vulnerability in Cybozu Remote Service 3.0.0 to 3.1.8 allows remote attackers to execute Java code file on the server via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16171 JVN MISC
cybozu -- remote_service	Directory traversal vulnerability in Cybozu Remote Service 3.0.0 to 3.1.8 for Windows allows remote authenticated attackers to read arbitrary files via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16170 JVN MISC
d-link -- multiple_devices	D-Link DIR-822 C1 before v3.11B01Beta, DIR-822-US C1 before v3.11B01Beta, DIR-850L A* before v1.21B08Beta, DIR-850L B* before v2.22B03Beta, and DIR-880L A* before v1.20B02Beta devices allow authentication bypass.	2019-01-08	not yet calculated	CVE-2018-20675 MISC
d-link -- multiple_devices	D-Link DIR-822 C1 before v3.11B01Beta, DIR-822-US C1 before v3.11B01Beta, DIR-850L A* before v1.21B08Beta, DIR-850L B* before v2.22B03Beta, and DIR-880L A* before v1.20B02Beta devices allow authenticated remote command execution.	2019-01-08	not yet calculated	CVE-2018-20674 MISC
digital_arts -- i-filter	HTTP header injection vulnerability in i-FILTER Ver.9.50R05 and earlier may allow remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks that may result in an arbitrary script injection or setting an arbitrary cookie values via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16181 MISC JVN
digital_arts -- i-filter	Cross-site scripting vulnerability in i-FILTER Ver.9.50R05 and earlier allows remote attackers to inject	2019-01-09	not yet	CVE-2018-16180

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary web script or HTML via unspecified vectors.		calculated	MISC JVN
django -- django	In Django 1.11.x before 1.11.18, 2.0.x before 2.0.10, and 2.1.x before 2.1.5, an Improper Neutralization of Special Elements in Output Used by a Downstream Component issue exists in django.views.defaults.page_not_found(), leading to content spoofing (in a 404 error page) if a user fails to recognize that a crafted URL has malicious content.	2019-01-09	not yet calculated	CVE-2019-3498 BID MISC MISC MLIST UBUNTU DEBIAN MISC
docker_engine -- docker_engine	Docker Engine before 18.09 allows attackers to cause a denial of service (dockerd memory consumption) via a large integer in a --cpuset-mems or --cpuset-cpus value, related to daemon/daemon_unix.go, pkg/parsers/parsers.go, and pkg/sysinfo/sysinfo.go.	2019-01-11	not yet calculated	CVE-2018-20699 MISC MISC
dokan -- dokan	Dokan, versions between 1.0.0.5000 and 1.2.0.1000, are vulnerable to a stack-based buffer overflow in the dokan1.sys driver. An attacker can create a device handle to the system driver and send arbitrary input that will trigger the vulnerability. This vulnerability was introduced in the 1.0.0.5000 version update.	2019-01-07	not yet calculated	CVE-2018-5410 BID MISC CONFIRM CERT-VN
elfinder -- elfinder	php/elFinder.class.php in elFinder before 2.1.45 leaks information if PHP's curl extension is enabled and safe_mode or open_basedir is not set.	2019-01-10	not yet calculated	CVE-2019-5884 MISC MISC
fork -- fork_cms	Fork CMS 5.0.6 allows stored XSS via the private/en/settings facebook_admin_ids parameter (aka "Admin ids" input in the Facebook section).	2019-01-09	not yet calculated	CVE-2018-20682 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
frog_cms -- frog_cms	Frog CMS 0.9.5 allows XSS via the forgot password page (aka the /admin/?/login/forgot URI).	2019-01-11	not yet calculated	CVE-2019-6243 MISC
frontaccounting -- frontaccounting	includes/db/class.reflines_db.inc in FrontAccounting 2.4.6 contains a SQL Injection vulnerability in the reference field that can allow the attacker to grab the entire database of the application via the void_transaction.php filterType parameter.	2019-01-08	not yet calculated	CVE-2019-5720 MISC
frrouting -- frrouting	bgpd in FRRouting FRR (aka Free Range Routing) 2.x and 3.x before 3.0.4, 4.x before 4.0.1, 5.x before 5.0.2, and 6.x before 6.0.2 (not affecting Cumulus Linux or VyOS), when ENABLE_BGP_VNC is used for Virtual Network Control, allows remote attackers to cause a denial of service (peering session flap) via attribute 255 in a BGP UPDATE packet. This occurred during Disco in January 2019 because FRR does not implement RFC 7606, and therefore the packets with 255 were considered invalid VNC data and the BGP session was closed.	2019-01-10	not yet calculated	CVE-2019-5892 CONFIRM MISC MISC MISC MISC MISC MISC
gitolite -- gitolite	commands/rsync in Gitolite before 3.6.11, if .gitolite.rc enables rsync, mishandles the rsync command line, which allows attackers to have a "bad" impact by triggering use of an option other than -v, -n, -q, or -P.	2019-01-09	not yet calculated	CVE-2018-20683 MISC MISC MISC MISC
gnu -- binutils	load_specific_debug_section in objdump.c in GNU Binutils through 2.31.1 contains an integer overflow vulnerability that can trigger a heap-based buffer overflow via a crafted section size.	2019-01-04	not yet calculated	CVE-2018-20671 BID MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gnu -- binutils	The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.	2019-01-04	not yet calculated	CVE-2018-20673 BID MISC
google -- chrome	The default selected dialog button in CustomHandlers in Google Chrome prior to 69.0.3497.81 allowed a remote attacker who convinced the user to perform certain operations to open external programs via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-16084 BID REDHAT CONFIRM MISC GENTOO
google -- chrome	Failure to prevent navigation to top frame to data URLs in Navigation in Google Chrome on iOS prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of the current page via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-20069 CONFIRM MISC
google -- chrome	Incorrect handling of 304 status codes in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of the current page via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-20068 CONFIRM MISC
google -- chrome	A renderer initiated back navigation was incorrectly allowed to cancel a browser initiated one in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of the current page via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-20067 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Incorrect object lifecycle in Extensions in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-20066 CONFIRM MISC
google -- chrome	Handling of URI action in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to initiate potentially unsafe navigations without a user gesture via a crafted PDF file.	2019-01-09	not yet calculated	CVE-2018-20065 CONFIRM MISC
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	CVE-2018-6166 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	CVE-2018-6163 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Incorrect handling of reloads in Navigation in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to spoof the contents of the	2019-01-09	not yet calculated	CVE-2018-6165 BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Omnibox (URL bar) via a crafted HTML page.			REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Insufficient origin checks for CSS content in Blink in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6164 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Improper deserialization in WebGL in Google Chrome on Mac prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6162 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	A heap buffer overflow in GPU in Google Chrome prior to 70.0.3538.67 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-17470 BID REDHAT CONF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				IRM MISC GENTOO DEBIAN
google -- chrome	An out of bounds read in PDFium in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.	2019-01-09	not yet calculated	CVE-2018-17461 CONFIRM MISC
google -- chrome	Incorrect handling of clicks in the omnibox in Navigation in Google Chrome prior to 69.0.3497.92 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-17459 REDHAT CONFIRM MISC
google -- chrome	An improper update of the WebAssembly dispatch table in WebAssembly in Google Chrome prior to 69.0.3497.92 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-17458 REDHAT CONFIRM MISC
google -- chrome	An object lifecycle issue in Blink could lead to a use after free in WebAudio in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-17457 CONFIRM MISC
google -- chrome	JavaScript alert handling in Prompts in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6160 BID CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				GENTOO
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.	2019-01-09	not yet calculated	CVE-2018-20070 CONFIRM MISC
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	CVE-2018-6167 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Insufficiently strict origin checks during JIT payment app installation in Payments in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to install a service worker for a domain that can host attacker controled files via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-20071 CONFIRM MISC
google -- chrome	Insufficient data validation in V8 builtins string generator could lead to out of bounds read and write access in V8 in Google Chrome prior to 62.0.3202.94 and allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2017-15428 CONFIRM MISC
google -- chrome	A missing check for whether a property of a JS object is private in V8 in Google Chrome prior to 55.0.2883.75 allowed a remote	2019-01-09	not yet calculated	CVE-2016-9651 REDH

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to execute arbitrary code inside a sandbox via a crafted HTML page.			AT BID CONFIRM MISC GENTOO EXPLOIT-DB
google -- chrome	A memory corruption bug in WebAssembly could lead to out of bounds read and write through V8 in WebAssembly in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2017-15401 CONFIRM MISC
google -- chrome	Using an ID that can be controlled by a compromised renderer which allows any frame to overwrite the page_state of any other frame in the same process in Navigation in Google Chrome on Chrome OS prior to 62.0.3202.74 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2017-15402 CONFIRM MISC
google -- chrome	Insufficient data validation in crosh could lead to a command injection under chronos privileges in Networking in Google Chrome on Chrome OS prior to 61.0.3163.113 allowed a local attacker to execute arbitrary code via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2017-15403 CONFIRM MISC
google -- chrome	An ability to process crash dumps under root privileges and inappropriate symlinks handling could lead to a local privilege escalation in Crash Reporting in	2019-01-09	not yet calculated	CVE-2017-15404 CONF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Google Chrome on Chrome OS prior to 61.0.3163.113 allowed a local attacker to perform privilege escalation via a crafted HTML page.			IRM MISC
google -- chrome	Inappropriate symlink handling and a race condition in the stateful recovery feature implementation could lead to a persistance established by a malicious code running with root privileges in cryptohomed in Google Chrome on Chrome OS prior to 61.0.3163.113 allowed a local attacker to execute arbitrary code via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2017-15405 CONF IRM MISC
google -- chrome	Insufficient enforcement of file access permission in the activeTab case in Extensions in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system via a crafted Chrome Extension.	2019-01-09	not yet calculated	CVE-2018-6179 BID REDHAT CONF IRM MISC GENTOO DEBIAN
google -- chrome	A precision error in Skia in Google Chrome prior to 68.0.3440.75 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6153 BID REDHAT CONF IRM MISC GENTOO DEBIAN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Eliding from the wrong side in an infobar in DevTools in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to Hide Chrome Security UI via a crafted Chrome Extension.	2019-01-09	not yet calculated	CVE-2018-6178 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	CVE-2018-6175 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Integer overflows in Swiftshader in Google Chrome prior to 68.0.3440.75 potentially allowed a remote attacker to execute arbitrary code via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6174 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to	2019-01-09	not yet	CVE-2018-6173

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.		calculated	BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	CVE-2018-6172 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	A bad cast in PDFium in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2019-01-09	not yet calculated	CVE-2018-6170 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Lack of timeout on extension install prompt in Extensions in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to trigger installation of an unwanted extension via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6169 BID REDHAT

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM MISC GENTOO DEBIAN
google -- chrome	A race condition in Oilpan in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6158 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Bad cast in DevTools in Google Chrome on Win, Linux, Mac, Chrome OS prior to 66.0.3359.117 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted Chrome Extension.	2019-01-09	not yet calculated	CVE-2018-6151 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	A use after free in ResourceCoordinator in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-16085 BID REDHAT CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				GENTOO
google -- chrome	A missing check for popup window handling in Fullscreen in Google Chrome on macOS prior to 69.0.3497.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-16080 BID REDHAT CONFIRM MISC GENTOO
google -- chrome	Unsafe handling of credit card details in Autofill in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-16078 BID REDHAT CONFIRM MISC GENTOO
google -- chrome	Incorrect handling of asynchronous methods in Fullscreen in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to enter full screen without showing a warning via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6097 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	A race condition between permission prompts and navigations in Prompts in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to spoof the contents of the	2019-01-09	not yet calculated	CVE-2018-16079 BID REDH

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Omnibox (URL bar) via a crafted HTML page.			AT CONFIRM MISC GENTOO
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	CVE-2018-6100 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	An asynchronous generator may return an incorrect state in V8 in Google Chrome prior to 66.0.3359.117 allowing a remote attacker to potentially exploit object corruption via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6106 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	readAsText() can indefinitely read the file picked by the user, rather than only once at the time the file is picked in File API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to access data on the user file system without explicit consent via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6109 BID REDHAT CONFIRM MISC GENT

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				OO DEBIAN
google -- chrome	Parsing documents as HTML in Downloads in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to cause Chrome to execute scripts via a local non-HTML page.	2019-01-09	not yet calculated	CVE-2018-6110 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	An object lifetime issue in the developer tools network handler in Google Chrome prior to 66.0.3359.117 allowed a local attacker to execute arbitrary code via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6111 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Allowing the chrome.debugger API to run on file:// URLs in DevTools in Google Chrome prior to 69.0.3497.81 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system without file access permission via a crafted Chrome Extension.	2019-01-09	not yet calculated	CVE-2018-16081 BID REDHAT CONFIRM MISC GENTOO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	A JavaScript focused window could overlap the fullscreen notification in Fullscreen in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6096 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	An out of bounds read in Swiftshader in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-16082 BID REDHAT CONFIRM MISC GENTOO
google -- chrome	An out of bounds read in forward error correction code in WebRTC in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-16083 BID REDHAT CONFIRM MISC GENTOO EXPLOIT-DB
google -- chrome	Making URLs clickable and allowing them to be styled in DevTools in Google Chrome prior to 66.0.3359.117 allowed a remote	2019-01-09	not yet calculated	CVE-2018-6112 BID

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to bypass navigation restrictions via a crafted HTML page.			REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Improper handling of pending navigation entries in Navigation in Google Chrome on iOS prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6113 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Incorrect enforcement of CSP for <object> tags in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6114 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Confusing settings in Autofill in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6117 BID REDHAT CONF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				IRM MISC GENTOO DEBIAN
google -- chrome	An integer overflow that could lead to an attacker-controlled heap out-of-bounds write in PDFium in Google Chrome prior to 66.0.3359.170 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.	2019-01-09	not yet calculated	CVE-2018-6120 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	A missing check for JS-simulated input events in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to download arbitrary files with no user input via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-16088 REDHAT CONFIRM MISC GENTOO
google -- chrome	Lack of proper state tracking in Permissions in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-16087 REDHAT CONFIRM MISC GENTOO
google -- chrome	Missing bounds check in PDFium in Google Chrome prior to 69.0.3497.81 allowed a remote	2019-01-09	not yet	CVE-2018-16076

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to perform an out of bounds memory read via a crafted PDF file.		calculated	BID REDHAT CONFIRM MISC GENTOO
google -- chrome	Insufficient origin checks in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6093 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Lack of secure text entry mode in Browser UI in Google Chrome on Mac prior to 67.0.3396.62 allowed a local attacker to obtain potentially sensitive information from process memory via a local process.	2019-01-09	not yet calculated	CVE-2018-6147 BID SECTRACK REDHAT CONFIRM MISC DEBIAN
google -- chrome	Early free of object in use in IndexDB in Google Chrome prior to 67.0.3396.62 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6127 BID SECTRACK

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				REDHAT CONFIRM MISC DEBIAN
google -- chrome	Off-by-one error in PDFium in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted PDF file.	2019-01-09	not yet calculated	CVE-2018-6144 BID SECTRACK REDHAT CONFIRM MISC DEBIAN
google -- chrome	Insufficient validation in V8 in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6143 BID SECTRACK REDHAT CONFIRM MISC DEBIAN
google -- chrome	Insufficient validation of an image filter in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory read via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6141 BID SECTRACK

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				REDHAT CONFIRM MISC DEBIAN
google -- chrome	Allowing the chrome.debugger API to attach to Web UI pages in DevTools in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.	2019-01-09	not yet calculated	CVE-2018-6140 BID SECTRACK REDHAT CONFIRM MISC DEBIAN
google -- chrome	Insufficient target checks on the chrome.debugger API in DevTools in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.	2019-01-09	not yet calculated	CVE-2018-6139 BID SECTRACK REDHAT CONFIRM MISC DEBIAN
google -- chrome	CSS Paint API in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6137 BID SECTRACK

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				REDHAT CONFIRM MISC DEBIAN
google -- chrome	Lack of clearing the previous site before loading alerts from a new one in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6135 BID SECTRACK REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	CVE-2018-6133 BID SECTRACK REDHAT CONFIRM MISC DEBIAN
google -- chrome	A precision error in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6126 BID BID SECTRAC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				K SECTRAC K REDHAT REDHAT REDHAT CONFIRM MISC GENTOO DEBIAN DEBIAN EXPLOIT-DB
google -- chrome	Service Workers can intercept any request made by an <embed> or <object> tag in Fetch API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6091 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Type confusion in ReadableStreams in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6124 BID SECTRAC K

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				REDHAT CONFIRM MISC DEBIAN
google -- chrome	A use after free in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6123 BID SECTRACK REDHAT CONFIRM MISC DEBIAN
google -- chrome	A Javascript reentrancy issues that caused a use-after-free in V8 in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-16065 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	A use after free in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-16066 BID REDHAT CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC GENTOO DEBIAN
google -- chrome	Missing validation in Mojo in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-16068 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	A use after free in WebRTC in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.	2019-01-09	not yet calculated	CVE-2018-16071 BID REDHAT CONFIRM MISC GENTOO EXPLOIT-DB
google -- chrome	A missing origin check related to HLS manifests in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass same origin policy via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-16072 BID CONFIRM MISC GENTOO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Type confusion could lead to a heap out-of-bounds write in V8 in Google Chrome prior to 64.0.3282.168 allowing a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-6056 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Insufficiently sanitized distributed objects in Updater in Google Chrome on macOS prior to 66.0.3359.117 allowed a local attacker to execute arbitrary code via an executable file.	2019-01-09	not yet calculated	CVE-2018-6084 BID BID CONFIRM MISC EXPLOIT-DB
google -- chrome	A use after free in WebAudio in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	CVE-2018-16067 BID REDHAT CONFIRM MISC GENTOO DEBIAN
google -- chrome	Insufficient data validation on image data in PDFium in Google Chrome prior to 51.0.2704.63 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.	2019-01-09	not yet calculated	CVE-2016-10403 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- api_connect	IBM API Connect 5.0.0.0 through 5.0.8.4 is affected by a vulnerability in the role-based access control in the management server that could allow an authenticated user to obtain highly sensitive information. IBM X-Force ID: 153175.	2019-01-08	not yet calculated	CVE-2018-1932 CONFIRM BID XF
ibm -- i_access_for_windows	An untrusted search path vulnerability in IBM i Access for Windows versions 7.1 and earlier on Windows can allow arbitrary code execution via a Trojan horse DLL in the current working directory, related to use of the LoadLibrary function. IBM X-Force ID: 152079.	2019-01-04	not yet calculated	CVE-2018-1888 BID XF CONFIRM
ibm -- jazz_reporting_service	IBM Jazz Reporting Service (JRS) 6.0.3, 6.0.4, 6.0.5, and 6.0.6 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: 152785.	2019-01-08	not yet calculated	CVE-2018-1918 CONFIRM BID XF
ibm -- spectrum_scale	IBM Spectrum Scale (GPFS) 4.1.1, 4.2.0, 4.2.1, 4.2.2, 4.2.3, and 5.0.0 where the use of Local Read Only Cache (LROC) is enabled may caused read operation on a file to return data from a different file. IBM X-Force ID: 154440.	2019-01-08	not yet calculated	CVE-2018-1993 BID XF CONFIRM
imperva -- securesphere	Imperva SecureSphere running v12.0.0.50 is vulnerable to local arbitrary code execution, escaping sealed-mode.	2019-01-10	not yet calculated	CVE-2018-5412 EXPLOIT-DB
imperva -- securesphere	Imperva SecureSphere running v13.0, v12.0, or v11.5 allows low privileged users to add SSH login	2019-01-10	not yet calculated	CVE-2018-5413 EXPL

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	keys to the admin user, resulting in privilege escalation.			OIT-DB
imperva -- securesphere_gateway	Imperva SecureSphere gateway (GW) running v13, for both pre-First Time Login or post-First Time Login (FTL), if the attacker knows the basic authentication passwords, the GW may be vulnerable to RCE through specially crafted requests, from the web access management interface.	2019-01-10	not yet calculated	CVE-2018-5403 EXPL OIT-DB
intel -- nuc_firmware	Improper setting of device configuration in system firmware for Intel(R) NUC kits may allow a privileged user to potentially enable escalation of privilege via physical access.	2019-01-10	not yet calculated	CVE-2017-3718 CONF IRM
intel -- optane_ssd_dc_p4800x	Firmware update routine in bootloader for Intel(R) Optane(TM) SSD DC P4800X before version E2010435 may allow a privileged user to potentially enable a denial of service via local access.	2019-01-10	not yet calculated	CVE-2018-12167 CONF IRM
intel -- optane_ssd_dc_p4800x	Insufficient write protection in firmware for Intel(R) Optane(TM) SSD DC P4800X before version E2010435 may allow a privileged user to potentially enable a denial of service via local access.	2019-01-10	not yet calculated	CVE-2018-12166 CONF IRM
intel -- proset/wireless_wifi_software	Improper directory permissions in the ZeroConfig service in Intel(R) PROSet/Wireless WiFi Software before version 20.90.0.7 may allow an authorized user to potentially enable escalation of privilege via local access.	2019-01-10	not yet calculated	CVE-2018-12177 CONF IRM
intel -- sgx_sdk_and_platform_software_for_window	Improper file verification in install routine for Intel(R) SGX SDK and Platform Software for Windows before 2.2.100 may allow an escalation of privilege via local access.	2019-01-10	not yet calculated	CVE-2018-18098 CONF IRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
intel -- ssd_data_center_tool_for_windows	Improper directory permissions in the installer for the Intel(R) SSD Data Center Tool for Windows before v3.0.17 may allow authenticated users to potentially enable an escalation of privilege via local access.	2019-01-10	not yet calculated	CVE-2018-3703 CONFIRM
intel -- system_support_utility_for_windows	Insufficient path checking in Intel(R) System Support Utility for Windows before 2.5.0.15 may allow an authenticated user to potentially enable an escalation of privilege via local access.	2019-01-10	not yet calculated	CVE-2019-0088 CONFIRM
irssi -- irssi	Irssi 1.1.x before 1.1.2 has a use after free when hidden lines are expired from the scroll buffer.	2019-01-09	not yet calculated	CVE-2019-5882 MISC MISC MISC
japan_atomic_energy_agency -- mapping_tool	Untrusted search path vulnerability in Installer of Mapping Tool 2.0.1.6 and 2.0.1.7 allows remote attackers to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-01-09	not yet calculated	CVE-2018-16176 MISC JVN
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins Jira Plugin 3.0.1 and earlier in JiraSite.java that allows attackers with Overall/Read access to have Jenkins connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-01-09	not yet calculated	CVE-2018-1000412 CONFIRM
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins Crowd 2 Integration Plugin 2.0.0 and earlier in CrowdSecurityRealm.java that allows attackers to have Jenkins perform a connection test, connecting to an attacker-specified	2019-01-09	not yet calculated	CVE-2018-1000422 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	server with attacker-specified credentials and connection settings.			
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier in core/src/main/java/hudson/model/Api.java that allows attackers to specify URLs to Jenkins that result in rendering arbitrary attacker-controlled HTML by Jenkins.	2019-01-09	not yet calculated	CVE-2018-1000407 CONFIRM
jenkins -- jenkins	A denial of service vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier in core/src/main/java/hudson/security/HudsonPrivateSecurityRealm.java that allows attackers without Overall/Read permission to access a specific URL on instances using the built-in Jenkins user database security realm that results in the creation of an ephemeral user record in memory.	2019-01-09	not yet calculated	CVE-2018-1000408 CONFIRM
jenkins -- jenkins	A session fixation vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier in core/src/main/java/hudson/security/HudsonPrivateSecurityRealm.java that prevented Jenkins from invalidating the existing session and creating a new one when a user signed up for a new user account.	2019-01-09	not yet calculated	CVE-2018-1000409 CONFIRM
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins Git Changelog Plugin 2.6 and earlier in GitChangelogSummaryDecorator/summary.jelly, GitChangelogLeftsideBuildDecorator/badge.jelly, GitLogJiraFilterPostPublisher/config.jelly, GitLogBasicChangelogPostPublisher/config.jelly that allows attackers	2019-01-09	not yet calculated	CVE-2018-1000426 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	able to control the Git history parsed by the plugin to have Jenkins render arbitrary HTML on some pages.			
jenkins -- jenkins	An insufficiently protected credentials vulnerability exists in Jenkins SonarQube Scanner Plugin 2.8 and earlier in SonarInstallation.java that allows attackers with local file system access to obtain the credentials used to connect to SonarQube.	2019-01-09	not yet calculated	CVE-2018-1000425 CONFIRM
jenkins -- jenkins	An insufficiently protected credentials vulnerability exists in Jenkins Crowd 2 Integration Plugin 2.0.0 and earlier in CrowdSecurityRealm.java, CrowdConfigurationService.java that allows attackers with local file system access to obtain the credentials used to connect to Crowd 2.	2019-01-09	not yet calculated	CVE-2018-1000423 CONFIRM
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins Mesos Plugin 0.17.1 and earlier in MesosCloud.java that allows attackers with Overall/Read access to initiate a test connection to an attacker-specified Mesos server with attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-01-09	not yet calculated	CVE-2018-1000421 CONFIRM
jenkins -- jenkins	A cross-site request forgery vulnerability exists in Jenkins JUnit Plugin 1.25 and earlier in TestObject.java that allows setting the description of a test result.	2019-01-09	not yet calculated	CVE-2018-1000411 CONFIRM
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins Mesos Plugin 0.17.1 and earlier in MesosCloud.java that allows	2019-01-09	not yet calculated	CVE-2018-1000420

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers with Overall/Read access to obtain credentials IDs for credentials stored in Jenkins.			CONFIRM
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins HipChat Plugin 2.2.0 and earlier in HipChatNotifier.java that allows attackers with Overall/Read access to obtain credentials IDs for credentials stored in Jenkins.	2019-01-09	not yet calculated	CVE-2018-1000419 CONFIRM
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins HipChat Plugin 2.2.0 and earlier in HipChatNotifier.java that allows attackers with Overall/Read access to send test notifications to an attacker-specified HipChat server with attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-01-09	not yet calculated	CVE-2018-1000418 CONFIRM
jenkins -- jenkins	A cross-site request forgery vulnerability exists in Jenkins Email Extension Template Plugin 1.0 and earlier in ExtEmailTemplateManagement.java that allows creating or removing templates.	2019-01-09	not yet calculated	CVE-2018-1000417 CONFIRM
jenkins -- jenkins	A reflected cross-site scripting vulnerability exists in Jenkins Job Config History Plugin 2.18 and earlier in all Jelly files that shows arbitrary attacker-specified HTML in Jenkins to users with Job/Configure access.	2019-01-09	not yet calculated	CVE-2018-1000416 CONFIRM
jenkins -- jenkins	An information exposure vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier, and the Stapler framework used by these releases, in core/src/main/java/org/kohsuke/stapler/RequestImpl.java,	2019-01-09	not yet calculated	CVE-2018-1000410 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	core/src/main/java/hudson/model/Descriptor.java that allows attackers with Overall/Administer permission or access to the local file system to obtain credentials entered by users if the form submission could not be successfully processed.			
jenkins -- jenkins	A cross-site request forgery vulnerability exists in Jenkins Config File Provider Plugin 3.1 and earlier in ConfigFilesManagement.java, FolderConfigFileAction.java that allows creating and editing configuration file definitions.	2019-01-09	not yet calculated	CVE-2018-1000414 CONFIRM
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins Config File Provider Plugin 3.1 and earlier in configfiles.jelly, providerlist.jelly that allows users with the ability to configure configuration files to insert arbitrary HTML into some pages in Jenkins.	2019-01-09	not yet calculated	CVE-2018-1000413 CONFIRM
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins Rebuilder Plugin 1.28 and earlier in RebuildAction/BooleanParameterValue.jelly, RebuildAction/ExtendedChoiceParameterValue.jelly, RebuildAction/FileParameterValue.jelly, RebuildAction/LabelParameterValue.jelly, RebuildAction/ListSubversionTagsParameterValue.jelly, RebuildAction/MavenMetadataParameterValue.jelly, RebuildAction/NodeParameterValue.jelly, RebuildAction/PasswordParameterValue.jelly,	2019-01-09	not yet calculated	CVE-2018-1000415 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	RebuildAction/RandomStringParameterValue.jelly, RebuildAction/RunParameterValue.jelly, RebuildAction/StringParameterValue.jelly, RebuildAction/TextParameterValue.jelly, RebuildAction/ValidatingStringParameterValue.jelly that allows users with Job/Configuration permission to insert arbitrary HTML into rebuild forms.			
jenkins -- jenkins	An insufficiently protected credentials vulnerability exists in Jenkins Artifactory Plugin 2.16.1 and earlier in ArtifactoryBuilder.java, CredentialsConfig.java that allows attackers with local file system access to obtain old credentials configured for the plugin before it integrated with Credentials Plugin.	2019-01-09	not yet calculated	CVE-2018-1000424 CONFIRM
jenkins -- jenkins	A path traversal vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier in core/src/main/java/hudson/model/FileParameterValue.java that allows attackers with Job/Configure permission to define a file parameter with a file name outside the intended directory, resulting in an arbitrary file write on the Jenkins master when scheduling a build.	2019-01-09	not yet calculated	CVE-2018-1000406 CONFIRM
jpcert_coordination_center -- logontracer	LogonTracer 1.2.0 and earlier allows remote attackers to conduct Python code injection attacks via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16168 MISC MISC
jpcert_coordination_center -- logontracer	Cross-site scripting vulnerability in LogonTracer 1.2.0 and earlier allows remote attackers to inject arbitrary	2019-01-09	not yet	CVE-2018-16165

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	web script or HTML via unspecified vectors.		calculated	MISC MISC
jpcert_coordination_center -- logontracer	LogonTracer 1.2.0 and earlier allows remote attackers to conduct XML External Entity (XXE) attacks via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16166 MISC MISC
jpcert_coordination_center -- logontracer	LogonTracer 1.2.0 and earlier allows remote attackers to execute arbitrary OS commands via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16167 MISC MISC
lib60870 -- lib60870	An issue was discovered in lib60870 2.1.1. LinkLayer_setAddress in link_layer/link_layer.c has a NULL pointer dereference.	2019-01-11	not yet calculated	CVE-2019-6137 MISC
libiec61850 -- libiec61850	An issue has been found in libIEC61850 v1.3.1. Ethernet_setProtocolFilter in hal/ethernet/linux/ethernet_linux.c has a SEGV, as demonstrated by sv_subscriber_example.c and sv_subscriber.c.	2019-01-11	not yet calculated	CVE-2019-6136 MISC
libiec61850 -- libiec61850	An issue has been found in libIEC61850 v1.3.1. Memory_malloc and Memory_calloc in hal/memory/lib_memory.c have memory leaks when called from mms/iso_mms/common/mms_value.c, server/mms_mapping/mms_mapping.c, and server/mms_mapping/mms_sv.c (via common/string_utilities.c), as demonstrated by iec61850_9_2_LE_example.c.	2019-01-11	not yet calculated	CVE-2019-6138 MISC
libiec61850 -- libiec61850	An issue has been found in libIEC61850 v1.3.1. Memory_malloc in hal/memory/lib_memory.c has a memory leak when called from	2019-01-11	not yet calculated	CVE-2019-6135 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Asn1PrimitiveValue_create in mms/asn1/asn1_ber_primitive_value.c, as demonstrated by goose_publisher_example.c and iec61850_9_2_LE_example.c.			
libpng -- libpng	png_create_info_struct in png.c in libpng 1.6.36 has a memory leak, as demonstrated by pngcp.	2019-01-11	not yet calculated	CVE-2019-6129 MISC
libtiff -- libtiff	The TIFFFdOpen function in tif_unix.c in LibTIFF 4.0.10 has a memory leak, as demonstrated by pal2rgb.	2019-01-11	not yet calculated	CVE-2019-6128 MISC
linux -- linux_kernel	The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of the fincore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.	2019-01-07	not yet calculated	CVE-2019-5489 MISC BID MISC MISC MISC MISC
linux -- linux_kernel	EARCLINK ESPCMS-P8 has SQL injection in the install_pack/index.php?ac=Member&at=verifyAccount verify_key parameter. install_pack/espcms_public/espcms_db.php may allow retrieving sensitive information from the ESPCMS database.	2019-01-07	not yet calculated	CVE-2019-5488 MISC
lockon -- ec-cube	Open redirect vulnerability in EC-CUBE (EC-CUBE 3.0.0, EC-CUBE 3.0.1, EC-CUBE 3.0.2, EC-CUBE 3.0.3, EC-CUBE 3.0.4, EC-CUBE 3.0.5, EC-CUBE 3.0.6, EC-CUBE 3.0.7, EC-CUBE 3.0.8, EC-CUBE 3.0.9, EC-CUBE 3.0.10, EC-CUBE	2019-01-09	not yet calculated	CVE-2018-16191 JVN MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	3.0.11, EC-CUBE 3.0.12, EC-CUBE 3.0.12-p1, EC-CUBE 3.0.13, EC-CUBE 3.0.14, EC-CUBE 3.0.15, EC-CUBE 3.0.16) allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.			
mate_desktop_environment -- mate-screensaver	mate-screensaver before 1.20.2 in MATE Desktop Environment allows physically proximate attackers to view screen content and possibly control applications. By unplugging and re-plugging or power-cycling external output devices (such as additionally attached graphical outputs via HDMI, VGA, DVI, etc.) the content of a screensaver-locked session can be revealed. In some scenarios, the attacker can execute applications, such as by clicking with a mouse.	2019-01-09	not yet calculated	CVE-2018-20681 MISC MISC MISC MISC
mcafee -- web_gateway	Improper input validation in the proxy component of McAfee Web Gateway 7.8.2.0 and later allows remote attackers to cause a denial of service via a crafted HTTP request parameter.	2019-01-09	not yet calculated	CVE-2019-3581 CONFIRM
micronet -- inplc	INplc-RT 3.08 and earlier allows remote attackers to bypass authentication to execute an arbitrary command through the protocol-compliant traffic. This is a different vulnerability than CVE-2018-0670.	2019-01-09	not yet calculated	CVE-2018-0669 MISC JVN
micronet -- inplc	Buffer overflow in INplc-RT 3.08 and earlier allows remote attackers to cause denial-of-service (DoS) condition that may result in executing arbtrary code via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-0668 MISC JVN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
micronet -- inplc	Privilege escalation vulnerability in INplc-RT 3.08 and earlier allows an attacker with administrator rights to execute arbitrary code on the Windows system via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-0671 MISC JVN
micronet -- inplc	INplc-RT 3.08 and earlier allows remote attackers to bypass authentication to execute an arbitrary command through the protocol-compliant traffic. This is a different vulnerability than CVE-2018-0669.	2019-01-09	not yet calculated	CVE-2018-0670 MISC JVN
micronet -- inplc	Untrusted search path vulnerability in Installer of INplc SDK Express 3.08 and earlier and Installer of INplc SDK Pro+ 3.08 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-01-09	not yet calculated	CVE-2018-0667 MISC JVN
microsoft -- .net_framework	An information disclosure vulnerability exists in .NET Framework and .NET Core which allows bypassing Cross-origin Resource Sharing (CORS) configurations, aka ".NET Framework Information Disclosure Vulnerability." This affects Microsoft .NET Framework 2.0, Microsoft .NET Framework 3.0, Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2, Microsoft .NET Framework 4.5.2, Microsoft .NET Framework 4.6, Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2, Microsoft .NET Framework 4.7/4.7.1/4.7.2, .NET Core 2.1, Microsoft .NET Framework 4.7.1/4.7.2, Microsoft .NET Framework 3.5, Microsoft .NET Framework 3.5.1, Microsoft .NET Framework 4.6/4.6.1/4.6.2, .NET	2019-01-08	not yet calculated	CVE-2019-0545 BID REDHAT CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Core 2.2, Microsoft .NET Framework 4.7.2.			
microsoft -- asp.net_core	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka "ASP.NET Core Denial of Service Vulnerability." This affects ASP.NET Core 2.2, ASP.NET Core 2.1. This CVE ID is unique from CVE-2019-0564.	2019-01-08	not yet calculated	CVE-2019-0548 BID REDHAT CONFIRM
microsoft -- edge	An elevation of privilege vulnerability exists in Microsoft Edge Browser Broker COM object, aka "Microsoft Edge Elevation of Privilege Vulnerability." This affects Microsoft Edge.	2019-01-08	not yet calculated	CVE-2019-0566 BID CONFIRM
microsoft -- edge_and_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 affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2019-0539, CVE-2019-0567.	2019-01-08	not yet calculated	CVE-2019-0568 BID CONFIRM
microsoft -- edge_and_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 affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2019-0567, CVE-2019-0568.	2019-01-08	not yet calculated	CVE-2019-0539 BID CONFIRM
microsoft -- edge_and_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."	2019-01-08	not yet calculated	CVE-2019-0567 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2019-0539, CVE-2019-0568.			
microsoft -- exchange_server	A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka "Microsoft Exchange Memory Corruption Vulnerability." This affects Microsoft Exchange Server.	2019-01-08	not yet calculated	CVE-2019-0586 BID CONFIRM
microsoft -- exchange_server	An information disclosure vulnerability exists when the Microsoft Exchange PowerShell API grants calendar contributors more view permissions than intended, aka "Microsoft Exchange Information Disclosure Vulnerability." This affects Microsoft Exchange Server.	2019-01-08	not yet calculated	CVE-2019-0588 BID CONFIRM
microsoft -- multiple_products	An information disclosure vulnerability exists when Microsoft Word macro buttons are used improperly, aka "Microsoft Word Information Disclosure Vulnerability." This affects Microsoft Word, Office 365 ProPlus, Microsoft Office, Word.	2019-01-08	not yet calculated	CVE-2019-0561 BID CONFIRM
microsoft -- multiple_products	A remote code execution vulnerability exists in the way that the MSHTML engine inproperly validates input, aka "MSHTML Engine Remote Code Execution Vulnerability." This affects Microsoft Office, Microsoft Office Word Viewer, Internet Explorer 9, Internet Explorer 11, Microsoft Excel Viewer, Internet Explorer 10, Office 365 ProPlus.	2019-01-08	not yet calculated	CVE-2019-0541 BID CONFIRM
microsoft -- multiple_products	A remote code execution vulnerability exists in Microsoft Word software when it fails to	2019-01-08	not yet	CVE-2019-0585

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	properly handle objects in memory, aka "Microsoft Word Remote Code Execution Vulnerability." This affects Word, Microsoft Office, Microsoft Office Word Viewer, Office 365 ProPlus, Microsoft SharePoint, Microsoft Office Online Server, Microsoft Word, Microsoft SharePoint Server.		calculated	BID CONFIRM
microsoft -- multiple_products	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 affects Microsoft SharePoint Server, Microsoft SharePoint, Microsoft Business Productivity Servers. This CVE ID is unique from CVE-2019-0556, CVE-2019-0557.	2019-01-08	not yet calculated	CVE-2019-0558 BID CONFIRM
microsoft -- sharepoint	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 affects Microsoft SharePoint. This CVE ID is unique from CVE-2019-0557, CVE-2019-0558.	2019-01-08	not yet calculated	CVE-2019-0556 BID CONFIRM
microsoft -- sharepoint	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka "Microsoft SharePoint Elevation of Privilege Vulnerability." This affects Microsoft SharePoint Server, Microsoft SharePoint.	2019-01-08	not yet calculated	CVE-2019-0562 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- sharepoint	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 affects Microsoft SharePoint. This CVE ID is unique from CVE-2019-0556, CVE-2019-0558.	2019-01-08	not yet calculated	CVE-2019-0557 BID CONFIRM
microsoft -- skype_for_android	An elevation of privilege vulnerability exists when Skype for Andriod fails to properly handle specific authentication requests, aka "Skype for Android Elevation of Privilege Vulnerability." This affects Skype 8.35.	2019-01-08	not yet calculated	CVE-2019-0622 BID CONFIRM
microsoft -- visual_studio	A remote code execution vulnerability exists in Visual Studio when the C++ compiler improperly handles specific combinations of C++ constructs, aka "Visual Studio Remote Code Execution Vulnerability." This affects Microsoft Visual Studio.	2019-01-08	not yet calculated	CVE-2019-0546 BID CONFIRM
microsoft -- visual_studio	An information disclosure vulnerability exists when Visual Studio improperly discloses arbitrary file contents if the victim opens a malicious .vscontent file, aka "Microsoft Visual Studio Information Disclosure Vulnerability." This affects Microsoft Visual Studio.	2019-01-08	not yet calculated	CVE-2019-0537 BID CONFIRM
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Service Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10,	2019-01-08	not yet calculated	CVE-2019-0571 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Windows Server 2019, Windows 10 Servers. This CVE ID is unique from CVE-2019-0572, CVE-2019-0573, CVE-2019-0574.			
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka "Windows Runtime Elevation of Privilege Vulnerability." This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers.	2019-01-08	not yet calculated	CVE-2019-0570 BID CONFIRM
microsoft -- windows	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0536, CVE-2019-0549, CVE-2019-0554.	2019-01-08	not yet calculated	CVE-2019-0569 BID CONFIRM
microsoft -- windows	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 affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016,	2019-01-08	not yet calculated	CVE-2019-0538 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.			
microsoft -- windows	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 affects Windows 10 Servers, Windows 10, Windows Server 2019. This CVE ID is unique from CVE-2019-0551.	2019-01-08	not yet calculated	CVE-2019-0550 BID CONFIRM
microsoft -- windows	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0536, CVE-2019-0554, CVE-2019-0569.	2019-01-08	not yet calculated	CVE-2019-0549 BID CONFIRM
microsoft -- windows	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka "Microsoft Windows Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows	2019-01-08	not yet calculated	CVE-2019-0543 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.			
microsoft -- windows	An elevation of privilege vulnerability exists in the Microsoft XmlDocument class that could allow an attacker to escape from the AppContainer sandbox in the browser, aka "Microsoft XmlDocument Elevation of Privilege Vulnerability." This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers.	2019-01-08	not yet calculated	CVE-2019-0555 BID CONFIRM
microsoft -- windows	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0536, CVE-2019-0549, CVE-2019-0569.	2019-01-08	not yet calculated	CVE-2019-0554 BID CONFIRM
microsoft -- windows	An information disclosure vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory, aka "Windows Subsystem for Linux Information Disclosure Vulnerability." This affects Windows 10 Servers, Windows 10, Windows Server 2019.	2019-01-08	not yet calculated	CVE-2019-0553 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Service Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers. This CVE ID is unique from CVE-2019-0571, CVE-2019-0572, CVE-2019-0574.	2019-01-08	not yet calculated	CVE-2019-0573 BID CONFIRM
microsoft -- windows	An elevation of privilege exists in Windows COM Desktop Broker, aka "Windows COM Elevation of Privilege Vulnerability." This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers.	2019-01-08	not yet calculated	CVE-2019-0552 BID CONFIRM
microsoft -- windows	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 affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers. This CVE ID is unique from CVE-2019-0550.	2019-01-08	not yet calculated	CVE-2019-0551 BID CONFIRM
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Service Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10	2019-01-08	not yet calculated	CVE-2019-0572 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Servers. This CVE ID is unique from CVE-2019-0571, CVE-2019-0573, CVE-2019-0574.			
microsoft -- windows	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 affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	CVE-2019-0576 BID CONFIRM
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Service Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers. This CVE ID is unique from CVE-2019-0571, CVE-2019-0572, CVE-2019-0573.	2019-01-08	not yet calculated	CVE-2019-0574 BID CONFIRM
microsoft -- windows	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 affects	2019-01-08	not yet calculated	CVE-2019-0577 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.			
microsoft -- windows	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 affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	CVE-2019-0581 BID CONFIRM
microsoft -- windows	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 affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows	2019-01-08	not yet calculated	CVE-2019-0582 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0583, CVE-2019-0584.			
microsoft -- windows	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 affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	CVE-2019-0578 BID CONFIRM
microsoft -- windows	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 affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows	2019-01-08	not yet calculated	CVE-2019-0579 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.			
microsoft -- windows	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 affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	CVE-2019-0580 BID CONFIRM
microsoft -- windows	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 affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows	2019-01-08	not yet calculated	CVE-2019-0583 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0584.			
microsoft -- windows	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 affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583.	2019-01-08	not yet calculated	CVE-2019-0584 BID CONFIRM
microsoft -- windows	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 affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0538,	2019-01-08	not yet calculated	CVE-2019-0575 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.			
microsoft -- windows	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0549, CVE-2019-0554, CVE-2019-0569.	2019-01-08	not yet calculated	CVE-2019-0536 BID CONFIRM
mizuho_bank -- mizuho_direct_app_for_android	The Mizuho Direct App for Android version 3.13.0 and earlier does not verify server certificates, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2019-01-09	not yet calculated	CVE-2018-16179 MISC MISC
modulemd -- modulemd	modulemd 1.3.1 and earlier uses an unsafe function for processing externally provided data, leading to remote code execution.	2019-01-10	not yet calculated	CVE-2017-1002157 CONFIRM
nec -- aterm_wf1200cr_and_aterm_wg1200cr	Aterm WF1200CR and Aterm WG1200CR (Aterm WF1200CR firmware Ver1.1.1 and earlier, Aterm WG1200CR firmware Ver1.0.1 and earlier) allows an attacker on the same network segment to execute arbitrary OS commands via SOAP interface of UPnP.	2019-01-09	not yet calculated	CVE-2018-16195 MISC JVN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nec -- aterm_wf1200cr_and_aterm_wg1200cr	Aterm WF1200CR and Aterm WG1200CR (Aterm WF1200CR firmware Ver1.1.1 and earlier, Aterm WG1200CR firmware Ver1.0.1 and earlier) allow an attacker on the same network segment to obtain information registered on the device via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16192 MISC JVN
nec -- aterm_wf1200cr_and_aterm_wg1200cr	Cross-site scripting vulnerability in Aterm WF1200CR and Aterm WG1200CR (Aterm WF1200CR firmware Ver1.1.1 and earlier, Aterm WG1200CR firmware Ver1.0.1 and earlier) allows authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16193 MISC JVN
nec -- aterm_wf1200cr_and_aterm_wg1200cr	Aterm WF1200CR and Aterm WG1200CR (Aterm WF1200CR firmware Ver1.1.1 and earlier, Aterm WG1200CR firmware Ver1.0.1 and earlier) allows authenticated attackers to execute arbitrary OS commands via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16194 MISC JVN
nelson -- open_source_erp	Nelson Open Source ERP v6.3.1 allows SQL Injection via the db/utils/query/data.xml query parameter.	2019-01-10	not yet calculated	CVE-2019-5893 MISC EXPLOIT-DB
netapp -- oncommand_unified_manager_for_7-mode	OnCommand Unified Manager for 7-Mode (core package) prior to 5.2.4 uses cookies that lack the secure attribute in certain circumstances making it vulnerable to impersonation via man-in-the-middle (MITM) attacks.	2019-01-07	not yet calculated	CVE-2018-5481 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nippon_telegraph_and_telephone_west_corporation -- security_measures_tool	Untrusted search path vulnerability in The installer of Windows10 Fall Creators Update Modify module for Security Measures tool allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-01-09	not yet calculated	CVE-2018-16177 MISC JVN
npm -- cordova-plugin-ionic-webview	Directory traversal vulnerability in cordova-plugin-ionic-webview versions prior to 2.2.0 (not including 2.0.0-beta.0, 2.0.0-beta.1, 2.0.0-beta.2, and 2.1.0-0) allows remote attackers to access arbitrary files via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16202 MISC JVN MISC
openssh -- openssh	In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename.	2019-01-10	not yet calculated	CVE-2018-20685 BID MISC MISC
panasonic -- bn-sdwbp3_firmware	Buffer overflow in BN-SDWBP3 firmware version 1.0.9 and earlier allows an attacker on the same network segment to execute arbitrary code via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-0678 JVN MISC
panasonic -- bn-sdwbp3_firmware	BN-SDWBP3 firmware version 1.0.9 and earlier allows attacker with administrator rights on the same network segment to execute arbitrary OS commands via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-0677 JVN MISC
panasonic -- bn-sdwbp3_firmware	BN-SDWBP3 firmware version 1.0.9 and earlier allows an attacker on the same network segment to bypass authentication to access to the management screen and execute an arbitrary command via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-0676 JVN MISC
panasonic -- multiple_pcs	An unquoted search path vulnerability in some pre-installed applications on Panasonic PC run on Windows 7 (32bit), Windows 7	2019-01-09	not yet calculated	CVE-2018-16183

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(64bit), Windows 8 (64bit), Windows 8.1 (64bit), Windows 10 (64bit) delivered in or later than October 2009 allow local users to gain privileges via a Trojan horse executable file and execute arbitrary code with eleveted privileges.			JVN MISC
pgpool -- global_development_group_pgpooladmin	PgpoolAdmin 4.0 and earlier allows remote attackers to bypass the login authentication and obtain the administrative privilege of the PostgreSQL database via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16203 JVN MISC
phpscriptsmall.com -- advance_peer_to_peer_mlm_script	The Admin Panel of PHP Scripts Mall Advance Peer to Peer MLM Script v1.7.0 allows remote attackers to bypass intended access restrictions by directly navigating to admin/dashboard.php or admin/user.php, as demonstrated by disclosure of information about users and staff.	2019-01-11	not yet calculated	CVE-2019-6126 MISC
phpscriptsmall.com -- citysearch_/_hotfrog_/_gelbeseiten_clone_script	PHP Scripts Mall Citysearch / Hotfrog / Gelbeseiten Clone Script 2.0.1 has Reflected XSS via the srch parameter, as demonstrated by restaurants-details.php.	2019-01-12	not yet calculated	CVE-2019-6248 MISC
pivotal -- concourse	Pivotal Concourse, all versions prior to 4.2.2, puts the user access token in a url during the login flow. A remote attacker who gains access to a user's browser history could obtain the access token and use it to authenticate as the user.	2019-01-11	not yet calculated	CVE-2019-3803 CONFIRM
policykit -- policykit	In PolicyKit (aka polkit) 0.115, the "start time" protection mechanism can be bypassed because fork() is not atomic, and therefore authorization decisions are improperly cached. This is related to lack of uid checking in	2019-01-11	not yet calculated	CVE-2019-6133 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	polkitbackend/polkitbackendinteractiveauthority.c.			
qibosoft -- qibosoft	qibosoft through V7 allows remote attackers to read arbitrary files via the member/index.php main parameter, as demonstrated by SSRF to a URL on the same web site to read a .sql file.	2019-01-08	not yet calculated	CVE-2019-5725 MISC
rakuten_securities -- market_speed	Untrusted search path vulnerability in the installer of MARKET SPEED Ver.16.4 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-01-09	not yet calculated	CVE-2018-16182 JVN MISC
red_hat -- satellite	A cross-site scripting (XSS) flaw was found in the katello component of Satellite. An attacker with privilege to create/edit organizations and locations is able to execute a XSS attacks against other users through the Subscriptions or the Red Hat Repositories wizards. This can possibly lead to malicious code execution and extraction of the anti-CSRF token of higher privileged users. Versions before 3.9.0 are vulnerable.	2019-01-12	not yet calculated	CVE-2018-16887 CONFIRM
ricoh -- interactive_whiteboard	RICOH Interactive Whiteboard D2200 V1.6 to V2.2, D5500 V1.6 to V2.2, D5510 V1.6 to V2.2, and the display versions with RICOH Interactive Whiteboard Controller Type1 V1.6 to V2.2 attached (D5520, D6500, D6510, D7500, D8400) allows remote attackers to execute arbitrary commands via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16184 JVN MISC
ricoh -- interactive_whiteboard	The RICOH Interactive Whiteboard D2200 V1.3 to V2.2, D5500 V1.3 to V2.2, D5510 V1.3 to V2.2, the display versions with RICOH Interactive Whiteboard Controller	2019-01-09	not yet calculated	CVE-2018-16187 JVN MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Type1 V1.3 to V2.2 attached (D5520, D6500, D6510, D7500, D8400), and the display versions with RICOH Interactive Whiteboard Controller Type2 V3.0 to V3.1.10137.0 attached (D5520, D6510, D7500, D8400) does not verify its server certificates, which allows man-in-the-middle attackers to eversdrop on encrypted communication.			
ricoh -- interactive_whiteboard	RICOH Interactive Whiteboard D2200 V1.1 to V2.2, D5500 V1.1 to V2.2, D5510 V1.1 to V2.2, the display versions with RICOH Interactive Whiteboard Controller Type1 V1.1 to V2.2 attached (D5520, D6500, D6510, D7500, D8400), and the display versions with RICOH Interactive Whiteboard Controller Type2 V3.0 to V3.1.10137.0 attached (D5520, D6510, D7500, D8400) uses hard-coded credentials, which may allow an attacker on the same network segments to login to the administrators settings screen and change the configuration.	2019-01-09	not yet calculated	CVE-2018-16186 JVN MISC
ricoh -- interactive_whiteboard	RICOH Interactive Whiteboard D2200 V1.1 to V2.2, D5500 V1.1 to V2.2, D5510 V1.1 to V2.2, the display versions with RICOH Interactive Whiteboard Controller Type1 V1.1 to V2.2 attached (D5520, D6500, D6510, D7500, D8400), and the display versions with RICOH Interactive Whiteboard Controller Type2 V3.0 to V3.1.10137.0 attached (D5520, D6510, D7500, D8400) allows remote attackers to execute a malicious program.	2019-01-09	not yet calculated	CVE-2018-16185 JVN MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ricoh -- interactive_whiteboard	SQL injection vulnerability in the RICOH Interactive Whiteboard D2200 V1.3 to V2.2, D5500 V1.3 to V2.2, D5510 V1.3 to V2.2, the display versions with RICOH Interactive Whiteboard Controller Type1 V1.3 to V2.2 attached (D5520, D6500, D6510, D7500, D8400), and the display versions with RICOH Interactive Whiteboard Controller Type2 V3.0 to V3.1.10137.0 attached (D5520, D6510, D7500, D8400) allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16188 JVN MISC
sap -- business_objects_mobile_for_android	SAP Business Objects Mobile for Android (before 6.3.5) application allows an attacker to provide malicious input in the form of a SAP BI link, preventing legitimate users from accessing the application by crashing it.	2019-01-08	not yet calculated	CVE-2019-0240 BID MISC MISC
sap -- bw/4hana	Under some circumstances, masterdata maintenance in SAP BW/4HANA (fixed in DW4CORE version 1.0 (SP08)) does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	2019-01-08	not yet calculated	CVE-2019-0243 BID MISC MISC
sap -- cloud_connector	SAP Cloud Connector, before version 2.11.3, allows an attacker to inject code that can be executed by the application. An attacker could thereby control the behavior of the application.	2019-01-08	not yet calculated	CVE-2019-0247 MISC MISC
sap -- cloud_connector	SAP Cloud Connector, before version 2.11.3, does not perform any authentication checks for functionalities that require user identity.	2019-01-08	not yet calculated	CVE-2019-0246 BID MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- commerce	SAP Commerce (previously known as SAP Hybris Commerce), before version 6.7, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-01-08	not yet calculated	CVE-2019-0238 BID MISC MISC
sap -- crm_webclient_ui	SAP CRM WebClient UI (fixed in SAPSCORE 1.12; S4FND 1.02; WEBCUIF 7.31, 7.46, 7.47, 7.48, 8.0, 8.01) does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-01-08	not yet calculated	CVE-2019-0244 BID MISC MISC
sap -- crm_webclient_ui	SAP CRM WebClient UI (fixed in SAPSCORE 1.12; S4FND 1.02; WEBCUIF 7.31, 7.46, 7.47, 7.48, 8.0, 8.01) does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-01-08	not yet calculated	CVE-2019-0245 BID MISC MISC
sap -- enterprise_financial_services	SAP Enterprise Financial Services (fixed in SAPSCORE 1.13, 1.14, 1.15; S4CORE 1.01, 1.02, 1.03; EA-FINSERV 1.10, 2.0, 5.0, 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0; Bank/CFM 4.63_20) does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	2019-01-08	not yet calculated	CVE-2018-2484 BID MISC MISC
sap -- financial_consolidation_cube_designer	A security weakness in SAP Financial Consolidation Cube Designer (BOBJ_EADES fixed in versions 8.0, 10.1) may allow an attacker to discover the password hash of an admin user.	2019-01-08	not yet calculated	CVE-2018-2499 BID MISC MISC
sap -- gateway_of_abap_application_server	Under certain conditions SAP Gateway of ABAP Application Server (fixed in SAP_GWFND 7.5, 7.51, 7.52, 7.53; SAP_BASIS 7.5) allows an attacker to access information which would otherwise be restricted.	2019-01-08	not yet calculated	CVE-2019-0248 BID MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- landscape_management	Under certain conditions SAP Landscape Management (VCM 3.0) allows an attacker to access information which would otherwise be restricted.	2019-01-08	not yet calculated	CVE-2019-0249 BID MISC MISC
sap -- work_and_inventory_manager	SAP Work and Inventory Manager (Agentry_SDK , before 7.0, 7.1) allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service.	2019-01-08	not yet calculated	CVE-2019-0241 BID MISC MISC
seiko_epson -- printers_and_scanners	HTTP header injection vulnerability in SEIKO EPSON printers and scanners (DS-570W firmware versions released prior to 2018 March 13, DS-780N firmware versions released prior to 2018 March 13, EP-10VA firmware versions released prior to 2017 September 4, EP-30VA firmware versions released prior to 2017 June 19, EP-707A firmware versions released prior to 2017 August 1, EP-708A firmware versions released prior to 2017 August 7, EP-709A firmware versions released prior to 2017 June 12, EP-777A firmware versions released prior to 2017 August 1, EP-807AB/AW/AR firmware versions released prior to 2017 August 1, EP-808AB/AW/AR firmware versions released prior to 2017 August 7, EP-879AB/AW/AR firmware versions released prior to 2017 June 12, EP-907F firmware versions released prior to 2017 August 1, EP-977A3 firmware versions released prior to 2017 August 1, EP-978A3 firmware versions released prior to 2017 August 7, EP-979A3 firmware	2019-01-09	not yet calculated	CVE-2018-0689 JVN MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	versions released prior to 2017 June 12, EP-M570T firmware versions released prior to 2017 September 6, EW-M5071FT firmware versions released prior to 2017 November 2, EW-M660FT firmware versions released prior to 2018 April 19, EW-M770T firmware versions released prior to 2017 September 6, PF-70 firmware versions released prior to 2018 April 20, PF-71 firmware versions released prior to 2017 July 18, PF-81 firmware versions released prior to 2017 September 14, PX-048A firmware versions released prior to 2017 July 4, PX-049A firmware versions released prior to 2017 September 11, PX-437A firmware versions released prior to 2017 July 24, PX-M350F firmware versions released prior to 2018 February 23, PX-M5040F firmware versions released prior to 2017 November 20, PX-M5041F firmware versions released prior to 2017 November 20, PX-M650A firmware versions released prior to 2017 October 17, PX-M650F firmware versions released prior to 2017 October 17, PX-M680F firmware versions released prior to 2017 June 29, PX-M7050F firmware versions released prior to 2017 October 13, PX-M7050FP firmware versions released prior to 2017 October 13, PX-M7050FX firmware versions released prior to 2017 November 7, PX-M7070FX firmware versions released prior to 2017 April 27, PX-M740F firmware versions released prior to 2017 December 4, PX-M741F firmware			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	versions released prior to 2017 December 4, PX-M780F firmware versions released prior to 2017 June 29, PX-M781F firmware versions released prior to 2017 June 27, PX-M840F firmware versions released prior to 2017 November 16, PX-M840FX firmware versions released prior to 2017 December 8, PX-M860F firmware versions released prior to 2017 October 25, PX-S05B/W firmware versions released prior to 2018 March 9, PX-S350 firmware versions released prior to 2018 February 23, PX-S5040 firmware versions released prior to 2017 November 20, PX-S7050 firmware versions released prior to 2018 February 21, PX-S7050PS firmware versions released prior to 2018 February 21, PX-S7050X firmware versions released prior to 2017 November 7, PX-S7070X firmware versions released prior to 2017 April 27, PX-S740 firmware versions released prior to 2017 December 3, PX-S840 firmware versions released prior to 2017 November 16, PX-S840X firmware versions released prior to 2017 December 8, PX-S860 firmware versions released prior to 2017 December 7) may allow a remote attackers to lead a user to a phishing site or execute an arbitrary script on the user's web browser.			
seiko_epson -- printers_and_scanners	Open redirect vulnerability in SEIKO EPSON printers and scanners (DS-570W firmware versions released prior to 2018 March 13, DS-780N firmware versions released prior to 2018	2019-01-09	not yet calculated	CVE-2018-0688 JVN MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	March 13, EP-10VA firmware versions released prior to 2017 September 4, EP-30VA firmware versions released prior to 2017 June 19, EP-707A firmware versions released prior to 2017 August 1, EP-708A firmware versions released prior to 2017 August 7, EP-709A firmware versions released prior to 2017 June 12, EP-777A firmware versions released prior to 2017 August 1, EP-807AB/AW/AR firmware versions released prior to 2017 August 1, EP-808AB/AW/AR firmware versions released prior to 2017 August 7, EP-879AB/AW/AR firmware versions released prior to 2017 June 12, EP-907F firmware versions released prior to 2017 August 1, EP-977A3 firmware versions released prior to 2017 August 1, EP-978A3 firmware versions released prior to 2017 August 7, EP-979A3 firmware versions released prior to 2017 June 12, EP-M570T firmware versions released prior to 2017 September 6, EW-M5071FT firmware versions released prior to 2017 November 2, EW-M660FT firmware versions released prior to 2018 April 19, EW-M770T firmware versions released prior to 2017 September 6, PF-70 firmware versions released prior to 2018 April 20, PF-71 firmware versions released prior to 2017 July 18, PF-81 firmware versions released prior to 2017 September 14, PX-048A firmware versions released prior to 2017 July 4, PX-049A firmware versions released prior to 2017 September 11, PX-437A			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	firmware versions released prior to 2017 July 24, PX-M350F firmware versions released prior to 2018 February 23, PX-M5040F firmware versions released prior to 2017 November 20, PX-M5041F firmware versions released prior to 2017 November 20, PX-M650A firmware versions released prior to 2017 October 17, PX-M650F firmware versions released prior to 2017 October 17, PX-M680F firmware versions released prior to 2017 June 29, PX-M7050F firmware versions released prior to 2017 October 13, PX-M7050FP firmware versions released prior to 2017 October 13, PX-M7050FX firmware versions released prior to 2017 November 7, PX-M7070FX firmware versions released prior to 2017 April 27, PX-M740F firmware versions released prior to 2017 December 4, PX-M741F firmware versions released prior to 2017 December 4, PX-M780F firmware versions released prior to 2017 June 29, PX-M781F firmware versions released prior to 2017 June 27, PX-M840F firmware versions released prior to 2017 November 16, PX-M840FX firmware versions released prior to 2017 December 8, PX-M860F firmware versions released prior to 2017 October 25, PX-S05B/W firmware versions released prior to 2018 March 9, PX-S350 firmware versions released prior to 2018 February 23, PX-S5040 firmware versions released prior to 2017 November 20, PX-S7050 firmware versions released prior to			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2018 February 21, PX-S7050PS firmware versions released prior to 2018 February 21, PX-S7050X firmware versions released prior to 2017 November 7, PX-S7070X firmware versions released prior to 2017 April 27, PX-S740 firmware versions released prior to 2017 December 3, PX-S840 firmware versions released prior to 2017 November 16, PX-S840X firmware versions released prior to 2017 December 8, PX-S860 firmware versions released prior to 2017 December 7) allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via the web interface of the affected product.			
shopxo -- shopxo	An issue was discovered in ShopXO 1.2.0. In the UnlinkDir method of the FileUtil.php file, the input parameters are not checked, resulting in input mishandling by the rmdir method. Attackers can delete arbitrary files by using "../" directory traversal.	2019-01-10	not yet calculated	CVE-2019-5887 MISC
shopxo -- shopxo	An issue was discovered in ShopXO 1.2.0. In the application\install\controller\Index.php file, there is no validation lock file in the Add method, which allows an attacker to reinstall the database. The attacker can write arbitrary code to database.php during system reinstallation.	2019-01-10	not yet calculated	CVE-2019-5886 MISC
svgpp -- svgpp	An issue was discovered in Anti-Grain Geometry (AGG) 2.4 as used in SVG++ (aka svgpp) 1.2.3. A heap-based buffer overflow bug in svgpp_agg_render may lead to code execution. In the	2019-01-12	not yet calculated	CVE-2019-6247 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	render_scanlines_aa_solid function, the blend_hline function is called repeatedly multiple times. blend_hline is equivalent to a loop containing write operations. Each call writes a piece of heap data, and multiple calls overwrite the data in the heap.			
svgpp -- svgpp	An issue was discovered in SVG++ (aka svgpp) 1.2.3. After calling the gil::get_color function in Generic Image Library in Boost, the return code is used as an address, leading to an Access Violation because of an out-of-bounds read.	2019-01-12	not yet calculated	CVE-2019-6246 MISC
svgpp -- svgpp	An issue was discovered in Anti-Grain Geometry (AGG) 2.4 as used in SVG++ (aka svgpp) 1.2.3. In the function agg::cell_aa::not_equal, dx is assigned to (x2 - x1). If dx >= dx_limit, which is (16384 << poly_subpixel_shift), this function will call itself recursively. There can be a situation where (x2 - x1) is always bigger than dx_limit during the recursion, leading to continual stack consumption.	2019-01-12	not yet calculated	CVE-2019-6245 MISC
systemd-journald -- systemd-journald	An out of bounds read was discovered in systemd-journald in the way it parses log messages that terminate with a colon ':'. A local attacker can use this flaw to disclose process memory data. Versions from v221 to v239 are vulnerable.	2019-01-11	not yet calculated	CVE-2018-16866 BID CONFIRM UBUNTU MISC
systemd-journald -- systemd-journald	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when many entries are sent to the journal socket. A local	2019-01-11	not yet calculated	CVE-2018-16865 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker, or a remote one if systemd-journal-remote is used, may use this flaw to crash systemd-journald or execute code with journald privileges. Versions through v240 are vulnerable.			UBUNTU MISC
systemd-journald -- systemd-journald	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when a program with long command line arguments calls syslog. A local attacker may use this flaw to crash systemd-journald or escalate his privileges. Versions through v240 are vulnerable.	2019-01-11	not yet calculated	CVE-2018-16864 BID CONFIRM UBUNTU MISC
toshiba -- toshiba_home_gateway_hem-gw16a_and_ hem-gw26a	Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier allows an attacker on the same network segment to bypass access restriction to access the information and files stored on the affected device.	2019-01-09	not yet calculated	CVE-2018-16197 MISC JVN
toshiba -- toshiba_home_gateway_hem-gw16a_and_ hem-gw26a	Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier may allow an attacker on the same network segment to access a non-documented developer screen to perform operations on the affected device.	2019-01-09	not yet calculated	CVE-2018-16198 MISC JVN
toshiba -- toshiba_home_gateway_hem-gw16a_and_ hem-gw26a	Cross-site scripting vulnerability in Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier allows an remote attacker to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16199 MISC JVN
toshiba -- toshiba_home_gateway_hem-gw16a_and_ hem-gw26a	Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9	2019-01-09	not yet	CVE-2018-16200

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and earlier allows an attacker on the same network segment to execute arbitrary OS commands.		calculated	MISC JVN
toshiba -- toshiba_home_gateway_hem-gw16a_and_ hem-gw26a	Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier uses hard-coded credentials, which may allow an attacker on the same network segment to login to the administrators settings screen and change the configuration or execute arbitrary OS commands.	2019-01-09	not yet calculated	CVE-2018-16201 MISC JVN
traccar -- traccar_server	In Traccar Server version 4.2, protocol/SpotProtocolDecoder.java might allow XXE attacks.	2019-01-09	not yet calculated	CVE-2019-5748 MISC MISC
usualtoolcms -- usualtoolcms	An issue was discovered in UsualToolCMS 8.0. cmsadmin/a_sqlbackx.php?t=sql allows CSRF attacks that can execute SQL statements, and consequently execute arbitrary PHP code by writing that code into a .php file.	2019-01-11	not yet calculated	CVE-2019-6244 MISC
weseek -- growi	Cross-site scripting vulnerability in GROWI v3.2.3 and earlier allows remote attackers to inject arbitrary web script or HTML via New Page modal.	2019-01-09	not yet calculated	CVE-2018-16205 JVN MISC
weseek -- growi	Cross-site scripting vulnerability in GROWI v3.2.3 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-0698 JVN MISC
windows -- dhcp_client	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka "Windows DHCP Client Remote Code Execution Vulnerability." This	2019-01-08	not yet calculated	CVE-2019-0547 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	affects Windows 10, Windows 10 Servers.			
winscp -- winscp	In WinSCP before 5.14 beta, due to missing validation, the scp implementation would accept arbitrary files sent by the server, potentially overwriting unrelated files. This affects TSCPFileSystem::SCPSink in core/ScpFileSystem.cpp.	2019-01-10	not yet calculated	CVE-2018-20684 BID MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.6.0 to 2.6.5 and 2.4.0 to 2.4.11, the RTSE dissector and other ASN.1 dissectors could crash. This was addressed in epan/charsets.c by adding a get_t61_string length check.	2019-01-08	not yet calculated	CVE-2019-5718 BID MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.6.0 to 2.6.5 and 2.4.0 to 2.4.11, the ISAKMP dissector could crash. This was addressed in epan/dissectors/packet-isakmp.c by properly handling the case of a missing decryption data block.	2019-01-08	not yet calculated	CVE-2019-5719 MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.6.0 to 2.6.5 and 2.4.0 to 2.4.11, the P_MUL dissector could crash. This was addressed in epan/dissectors/packet-p_mul.c by rejecting the invalid sequence number of zero.	2019-01-08	not yet calculated	CVE-2019-5717 BID MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.4.0 to 2.4.11, the ENIP dissector could crash. This was addressed in epan/dissectors/packet-enip.c by changing the memory-management approach so that a use-after-free is avoided.	2019-01-08	not yet calculated	CVE-2019-5721 MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.6.0 to 2.6.5, the 6LoWPAN dissector could crash. This was addressed in epan/dissectors/packet-6lowpan.c by	2019-01-08	not yet calculated	CVE-2019-5716 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	avoiding use of a TVB before its creation.			MISC MISC
wordpress -- wordpress	Cross-site scripting vulnerability in WordPress plugin spam-byebye 2.2.1 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-12	not yet calculated	CVE-2018-16206 JVN MISC
wordpress -- wordpress	SQL injection vulnerability in the LearnPress prior to version 3.1.0 allows attacker with administrator rights to execute arbitrary SQL commands via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16175 JVN MISC
wordpress -- wordpress	Open redirect vulnerability in LearnPress prior to version 3.1.0 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16174 JVN MISC
wordpress -- wordpress	Cross-site scripting vulnerability in LearnPress prior to version 3.1.0 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16173 JVN MISC
wordpress -- wordpress	The "Social Pug - Easy Social Share Buttons" plugin before 1.2.6 for WordPress allows XSS via the wp-admin/admin.php?page=dpsp-toolkit dpsp_message_class parameter.	2019-01-09	not yet calculated	CVE-2016-10736 MISC
wordpress -- wordpress	Cross-site scripting vulnerability in Event Calendar WD version 1.1.21 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16164 JVN MISC MISC MISC
wordpress -- wordpress	Cross-site scripting vulnerability in Google XML Sitemaps Version 4.0.9 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16204 JVN MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xiaocms -- xiaocms	An issue was discovered in XiaoCms 20141229. It allows admin/index.php?c=database table[] SQL injection. This can be used for PHP code execution via "INTO OUTFILE" with a .php filename.	2019-01-11	not yet calculated	CVE-2019-6127 MISC
xterm.js -- xterm.js	A remote code execution vulnerability exists in Xterm.js when the component mishandles special characters, aka "Xterm Remote Code Execution Vulnerability." This affects xterm.js.	2019-01-09	not yet calculated	CVE-2019-0542 BID MISC
yamaha -- multiple_routers	Yamaha routers RT57i Rev.8.00.95 and earlier, RT58i Rev.9.01.51 and earlier, NVR500 Rev.11.00.36 and earlier, RTX810 Rev.11.01.31 and earlier, allow an administrative user to embed arbitrary scripts to the configuration data through a certain form field of the configuration page, which may be executed on another administrative user's web browser. This is a different vulnerability from CVE-2018-0666.	2019-01-09	not yet calculated	CVE-2018-0665 MISC MISC JVN MISC
yamaha -- multiple_routers	Yamaha routers RT57i Rev.8.00.95 and earlier, RT58i Rev.9.01.51 and earlier, NVR500 Rev.11.00.36 and earlier, RTX810 Rev.11.01.31 and earlier, allow an administrative user to embed arbitrary scripts to the configuration data through a certain form field of the configuration page, which may be executed on another administrative user's web browser. This is a different vulnerability from CVE-2018-0665.	2019-01-09	not yet calculated	CVE-2018-0666 MISC MISC JVN MISC
yokogawa -- multiple_products	Buffer overflow in the license management function of YOKOGAWA products (iDefine for ProSafe-RS R1.16.3 and earlier, STARDOM VDS R7.50 and earlier, STARDOM FCN/FCJ Simulator	2019-01-09	not yet calculated	CVE-2018-0651 BID MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	R4.20 and earlier, ASTPLANNER R15.01 and earlier, TriFellows V5.04 and earlier) allows remote attackers to stop the license management function or execute an arbitrary program via unspecified vectors.			
yokogawa -- multiple_products	Multiple Yokogawa products that contain Vnet/IP Open Communication Driver (CENTUM CS 3000(R3.05.00 - R3.09.50), CENTUM CS 3000 Entry Class(R3.05.00 - R3.09.50), CENTUM VP(R4.01.00 - R6.03.10), CENTUM VP Entry Class(R4.01.00 - R6.03.10), Exaopc(R3.10.00 - R3.75.00), PRM(R2.06.00 - R3.31.00), ProSafe-RS(R1.02.00 - R4.02.00), FAST/TOOLS(R9.02.00 - R10.02.00), B/M9000 VP(R6.03.01 - R8.01.90)) allows remote attackers to cause a denial of service attack that may result in stopping Vnet/IP Open Communication Driver's communication via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16196 BID MISC MISC

Back to top