Vulnerability Summary for the Week of June 24, 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
cesanta -- mongoose	An issue was discovered in Mongoose before 6.15. The parse_mqtt() function in mg_mqtt.c has a critical heap-based buffer overflow.	2019-06-24	7.5	CVE-2019-12951 MISC MISC
cisco -- data_center_network_manager	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to bypass authentication and execute	2019-06-26	7.5	CVE-2019-1619 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary actions with administrative privileges on an affected device. The vulnerability is due to improper session management on affected DCNM software. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to gain administrative access on the affected device.			
cisco -- data_center_network_manager	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to upload arbitrary files on an affected device. The vulnerability is due to incorrect permission settings in affected DCNM software. An attacker could exploit this vulnerability by uploading specially crafted data to the affected device. A successful exploit could allow the attacker to write arbitrary files on the filesystem and execute code with root privileges on the affected device.	2019-06-26	10.0	CVE-2019-1620 BID CISCO
citrix -- appdna	Citrix AppDNA before 7 1906.1.0.472 has Incorrect Access Control.	2019-06-24	7.5	CVE-2019-12292 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- support_assistant	HP Support Assistant 8.7.50 and earlier allows a user to gain system privilege and allows unauthorized modification of directories or files. Note: A different vulnerability than CVE-2019-6329.	2019-06-25	7.2	CVE-2019-6328 BID CONFIRM
hp -- support_assistant	HP Support Assistant 8.7.50 and earlier allows a user to gain system privilege and allows unauthorized modification of directories or files. Note: A different vulnerability than CVE-2019-6328.	2019-06-25	7.2	CVE-2019-6329 BID CONFIRM
libexpat -- expat	In libexpat in Expat before 2.2.7, XML input including XML names that contain a large number of colons could make the XML parser consume a high amount of RAM and CPU resources while processing (enough to be usable for denial-of-service attacks).	2019-06-24	7.8	CVE-2018-20843 MISC MISC MISC MISC MISC MLIST BUGTRAQ UBUNTU UBUNTU DEBIAN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
livezilla -- livezilla	LiveZilla Server before 8.0.1.1 is vulnerable to SQL Injection in server.php via the p_ext_rse parameter.	2019-06-24	7.5	CVE-2019-12939 BID MISC
livezilla -- livezilla	LiveZilla Server before 8.0.1.1 is vulnerable to Denial Of Service (memory consumption) in knowledgebase.php via a large integer value of the depth parameter.	2019-06-24	7.1	CVE-2019-12940 MISC
livezilla -- livezilla	LiveZilla Server before 8.0.1.1 is vulnerable to SQL Injection in functions.internal.build.inc.php via the parameter p_dt_s_d.	2019-06-25	7.5	CVE-2019-12960 MISC
pivotal_software -- spring_security	Spring Security, versions 4.2.x up to 4.2.12, and older unsupported versions support plain text passwords using PlaintextPasswordEncoder. If an application using an affected version of Spring Security is leveraging PlaintextPasswordEncoder and a user has a null encoded password, a malicious user (or attacker) can authenticate using a password of "null".	2019-06-26	7.5	CVE-2019-11272 CONFIRM
postgresql -- postgresql	PostgreSQL versions 10.x before 10.9 and versions 11.x before 11.4 are vulnerable to a	2019-06-26	9.0	CVE-2019-10164

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	stack-based buffer overflow. Any authenticated user can overflow a stack-based buffer by changing the user's own password to a purpose-crafted value. This often suffices to execute arbitrary code as the PostgreSQL operating system account.			CONFIRM MISC
qemu -- qemu	The QMP migrate command in QEMU version 4.0.0 and earlier is vulnerable to OS command injection, which allows the remote attacker to achieve code execution, denial of service, or information disclosure by sending a crafted QMP command to the listening server.	2019-06-24	10.0	CVE-2019-12928 MISC
qemu -- qemu	The QMP guest_exec command in QEMU 4.0.0 and earlier is prone to OS command injection, which allows the attacker to achieve code execution, denial of service, or information disclosure by sending a crafted QMP command to the listening server.	2019-06-24	10.0	CVE-2019-12929 MISC
toaruos -- toaruos	apps/gsudo.c in gsudo in ToaruOS through 1.10.9 has a buffer overflow allowing local privilege escalation to the root user via the DISPLAY environment variable.	2019-06-23	7.2	CVE-2019-12937 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
analogic -- poste.io	The Roundcube component of Analogic Poste.io 2.1.6 uses .htaccess to protect the logs/ folder, which is effective with the Apache HTTP Server but is ineffective with nginx. Attackers can read logs via the webmail/logs/sendmail URI.	2019-06-24	4.0	CVE-2019-12938 MISC MISC
apache -- tomcat	The fix for CVE-2019-0199 was incomplete and did not address HTTP/2 connection window exhaustion on write in Apache Tomcat versions 9.0.0.M1 to 9.0.19 and 8.5.0 to 8.5.40 . By not sending WINDOW_UPDATE messages for the connection window (stream 0) clients were able to cause server-side threads to block eventually leading to thread exhaustion and a DoS.	2019-06-21	5.0	CVE-2019-10072 BID MISC CONFIRM CONFIRM CONFIRM
atlassian -- jira	The issue searching component in Jira before version 8.1.0 allows remote attackers to deny access to Jira service	2019-06-26	4.0	CVE-2019-11583

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	via denial of service vulnerability in issue search when ordering by "Epic Name".			BID MISC
bcnquark -- quarking_password_manager	BCN Quark Quarking Password Manager 3.1.84 suffers from a clickjacking vulnerability caused by allowing * within web_accessible_resources. An attacker can take advantage of this vulnerability and cause significant harm.	2019-06-24	4.3	CVE-2019-12880 MISC FULLDISC MISC
canonical -- ubuntu_linux	arch/powerpc/mm/mmu_context_book3s64.c in the Linux kernel before 5.1.15 for powerpc has a bug where unrelated processes may be able to read/write to one another's virtual memory under certain conditions via an mmap above 512 TB. Only a subset of powerpc systems are affected.	2019-06-25	6.9	CVE-2019-12817 MLIST BID CONFIRM MISC FEDORA UBUNTU
cisco -- data_center_network_manager	A vulnerability in the web-based management interface of Cisco Data	2019-06-26	5.0	CVE-2019-1621

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to gain access to sensitive files on an affected device. The vulnerability is due to incorrect permissions settings on affected DCNM software. An attacker could exploit this vulnerability by connecting to the web-based management interface of an affected device and requesting specific URLs. A successful exploit could allow the attacker to download arbitrary files from the underlying filesystem of the affected device.			BID CISCO
cisco -- data_center_network_manager	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to retrieve sensitive information from an affected device. The vulnerability is due to improper access controls for certain URLs on affected DCNM software. An attacker could exploit this vulnerability by connecting to the web-based	2019-06-26	5.0	CVE-2019-1622 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	management interface of an affected device and requesting specific URLs. A successful exploit could allow the attacker to download log files and diagnostic information from the affected device.			
dell -- supportassist_for_business_pcs	PC-Doctor Toolbox before 7.3 has an Uncontrolled Search Path Element.	2019-06-25	6.8	CVE-2019-12280 MISC FULLDISC CONFIRM BID MISC MISC MISC MISC
fasterxml -- jackson-databind	FasterXML jackson-databind 2.x before 2.9.9 might allow attackers to have a variety of impacts by leveraging failure to block the logback-core class from	2019-06-24	4.3	CVE-2019-12384 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	polymorphic deserialization. Depending on the classpath content, remote code execution may be possible.			MISC CONFIRM
glyphandcog -- xpdfreader	In Xpdf 4.01.01, a buffer over-read could be triggered in FoFiType1C::convertToType1 in fofi/FoFiType1C.cc when the index number is larger than the charset array bounds. It can, for example, be triggered by sending a crafted PDF document to the pdftops tool. It allows an attacker to use a crafted pdf file to cause Denial of Service or an information leak, or possibly have unspecified other impact.	2019-06-24	6.8	CVE-2019-12957 MISC
glyphandcog -- xpdfreader	In Xpdf 4.01.01, a heap-based buffer over-read could be triggered in FoFiType1C::convertToType0 in fofi/FoFiType1C.cc when it is trying to access the second privateDicts array element, because the privateDicts array has only one element allocated.	2019-06-24	4.3	CVE-2019-12958 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gnu -- binutils	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. There is a heap-based buffer over-read in _bfd_doprnt in bfd.c because elf_object_p in elfcode.h mishandles an e_shstrndx section of type SHT_GROUP by omitting a trailing '\0' character.	2019-06-26	4.3	CVE-2019-12972 BID MISC MISC
google -- chrome	Insufficient data validation in V8 in Google Chrome prior to 56.0.2924.76 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-06-27	4.3	CVE-2017-5028 MISC MISC
google -- chrome	Insufficient data validation in Extensions API in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.	2019-06-27	4.3	CVE-2018-16064 MISC MISC
google -- chrome	Unintended floating-point error accumulation in SwiftShader in Google	2019-06-27	4.3	CVE-2018-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Chrome prior to 69.0.3497.81 allowed a remote attacker to leak cross-origin data via a crafted HTML page.			16069 MISC MISC
google -- chrome	Insufficient data validation in filesystem URIs 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 domain name.	2019-06-27	4.3	CVE-2018-17460 MISC MISC
google -- chrome	Incorrect array position calculations in V8 in Google Chrome prior to 70.0.3538.102 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.	2019-06-27	6.8	CVE-2018-17478 MISC MISC
google -- chrome	Incorrect object lifetime calculations in GPU code in Google Chrome prior to 70.0.3538.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-06-27	6.8	CVE-2018-17479 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	A double-eviction in the Incognito mode cache that lead to a user-after-free in cache in Google Chrome prior to 66.0.3359.139 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page.	2019-06-27	6.8	CVE-2018-6118 MISC MISC
google -- chrome	Object lifecycle issue in WebAssembly in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-06-27	6.8	CVE-2018-6131 MISC MISC
google -- chrome	Uninitialized data in WebRTC in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted video file.	2019-06-27	4.3	CVE-2018-6132 MISC MISC
google -- chrome	Information leak in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to bypass no-referrer policy via a crafted HTML page.	2019-06-27	4.3	CVE-2018-6134 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Missing type check 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.	2019-06-27	4.3	CVE-2018-6136 MISC MISC
google -- chrome	Insufficient policy enforcement in Extensions API in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.	2019-06-27	5.8	CVE-2018-6138 MISC MISC
google -- chrome	Array bounds check failure 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 PDF file.	2019-06-27	4.3	CVE-2018-6142 MISC MISC
google -- chrome	Insufficient data validation in WebGL in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially	2019-06-27	6.8	CVE-2018-6154 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploit heap corruption via a crafted HTML page.			
google -- chrome	Incorect derivation of a packet length in WebRTC in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.	2019-06-27	6.8	CVE-2018-6156 MISC MISC
google -- chrome	Insufficient policy enforcement in Blink in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to bypass same origin policy via a crafted HTML page.	2019-06-27	6.8	CVE-2018-6161 MISC MISC
google -- chrome	Information leak in media engine in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2019-06-27	4.3	CVE-2018-6168 MISC MISC
google -- chrome	Insufficient file type enforcement in Extensions API in Google Chrome prior	2019-06-27	4.6	CVE-2018-6176

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to 68.0.3440.75 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted Chrome Extension.			MISC MISC
google -- chrome	Information leak in media engine in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-06-27	4.3	CVE-2018-6177 MISC MISC
google -- chrome	Use after free in Blink in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-06-27	6.8	CVE-2019-5808 SUSE MISC MISC FEDORA
google -- chrome	Use after free in file chooser in Google Chrome prior to 74.0.3729.108 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page.	2019-06-27	6.8	CVE-2019-5809 SUSE MISC MISC FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Information leak in autofill in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2019-06-27	4.3	CVE-2019-5810 SUSE MISC MISC FEDORA
google -- chrome	Use after free in V8 in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-06-27	6.8	CVE-2019-5813 SUSE MISC MISC FEDORA
google -- chrome	Incorrect security UI in popup blocker in Google Chrome on iOS prior to 75.0.3770.80 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2019-06-27	4.3	CVE-2019-5840 SUSE MISC MISC FEDORA
ibm -- api_connect	IBM API Connect 5.0.0.0 through 5.0.8.6 is vulnerable to cross-site request forgery which could allow an attacker to execute	2019-06-25	6.8	CVE-2018-1858 CONFIR

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 151256.			M BID XF
ibm -- api_connect	IBM API Connect 2018.1 through 2018.4.1.5 could allow an attacker to obtain sensitive information from a specially crafted HTTP request that could aid an attacker in further attacks against the system. IBM X-Force ID: 155150.	2019-06-25	5.0	CVE-2018-2011 BID XF CONFIRM
ibm -- api_connect	IBM API Connect 2018.1 through 2018.4.1.5 could disclose sensitive information to an unauthorized user that could aid in further attacks against the system. IBM X-Force ID: 155193.	2019-06-25	5.0	CVE-2018-2013 BID XF CONFIRM
ibm -- api_connect	IBM API Connect 5.0.0.0 through 5.0.8.6 could allow an unauthorized user to obtain sensitive information about the system users using specially crafted HTTP requests. IBM X-Force ID: 162162.	2019-06-25	5.0	CVE-2019-4382 BID XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- pureapplication_system	IBM PureApplication System 2.2.3.0 through 2.2.5.3 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 159240.	2019-06-26	6.5	CVE-2019-4224 XF CONFIRM
ibm -- pureapplication_system	IBM PureApplication System 2.2.3.0 through 2.2.5.3 weakness in the implementation of locking feature in pattern editor. An attacker by intercepting the subsequent requests can bypass business logic to modify the pattern to unlocked state. IBM X-Force ID: 159416.	2019-06-26	4.0	CVE-2019-4234 XF CONFIRM
ibm -- pureapplication_system	IBM PureApplication System 2.2.3.0 through 2.2.5.3 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 159417.	2019-06-26	5.0	CVE-2019-4235 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- pureapplication_system	IBM PureApplication System 2.2.3.0 through 2.2.5.3 could allow an authenticated user with local access to bypass authentication and obtain administrative access. IBM X-Force ID: 159467.	2019-06-26	4.6	CVE-2019-4241 XF CONFIRM
ibm -- rational_collaborative_lifecycle_management	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 discloses sensitive information in error messages that may be used by a malicious user to orchestrate further attacks. IBM X-Force ID: 147838.	2019-06-27	4.0	CVE-2018-1734 CONFIRM XF
ibm -- rational_collaborative_lifecycle_management	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) could allow an authenticated user to obtain sensitive information from CLM Applications that could be used in further attacks against the system. IBM X-Force ID: 157384.	2019-06-27	4.0	CVE-2019-4084 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- rational_collaborative_lifecycle_management	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 159883.	2019-06-27	5.0	CVE-2019-4252 CONFIRM XF
ibm -- security_access_manager	IBM Security Access Manager 9.0.1 through 9.0.6 is affected by a security vulnerability that could allow authenticated users to impersonate other users. IBM X-Force ID: 158331.	2019-06-25	6.5	CVE-2019-4135 XF CONFIRM
ibm -- security_access_manager	IBM Security Access Manager 9.0.1 through 9.0.6 does not validate, or incorrectly validates, a certificate which could allow an attacker to spoof a trusted entity by using a man-in-the-middle (MITM) attack. IBM X-Force ID: 158510.	2019-06-25	4.3	CVE-2019-4150 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_access_manager	IBM Security Access Manager 9.0.1 through 9.0.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 158512.	2019-06-25	4.3	CVE-2019-4151 XF CONFIRM
ibm -- security_access_manager	IBM Security Access Manager 9.0.1 through 9.0.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 158572.	2019-06-25	4.3	CVE-2019-4156 XF CONFIRM
ibm -- security_access_manager	IBM Security Access Manager 9.0.1 through 9.0.6 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: 158573.	2019-06-25	4.3	CVE-2019-4157 XF CONFIRM
ibm -- security_access_manager	IBM Security Access Manager 9.0.1 through 9.0.6 does not prove that a user's identity is correct which can lead to the	2019-06-25	5.5	CVE-2019-4158 XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exposure of resources or functionality to unintended actors. IBM X-Force ID: 158574.			CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator 6.0.0.0 and 6.0.0.1 reveals sensitive information from a stack trace that could be used in further attacks against the system. IBM X-Force ID: 162803.	2019-06-25	4.0	CVE-2019-4377 BID XF CONFIRM
imagemagick -- imagemagick	A NULL pointer dereference in the function ReadPANGOImage in coders/pango.c and the function ReadVIDImage in coders/vid.c in ImageMagick 7.0.8-34 allows remote attackers to cause a denial of service via a crafted image.	2019-06-26	4.3	CVE-2019-12974 BID MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-34 has a memory leak vulnerability in the WriteDPXImage function in coders/dpx.c.	2019-06-26	4.3	CVE-2019-12975 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
imagemagick -- imagemagick	ImageMagick 7.0.8-34 has a memory leak in the ReadPCLImage function in coders/pcl.c.	2019-06-26	4.3	CVE-2019-12976 BID MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-34 has a "use of uninitialized value" vulnerability in the WriteJP2Image function in coders/jp2.c.	2019-06-26	6.8	CVE-2019-12977 BID MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-34 has a "use of uninitialized value" vulnerability in the ReadPANGOImage function in coders/pango.c.	2019-06-26	6.8	CVE-2019-12978 BID MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-34 has a "use of uninitialized value" vulnerability in the SyncImageSettings function in MagickCore/image.c. This is related to AcquireImage in magick/image.c.	2019-06-26	6.8	CVE-2019-12979 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lenovo -- system_update	A denial of service vulnerability was reported in Lenovo System Update before version 5.07.0084 that could allow log files to be written to non-standard locations.	2019-06-26	5.0	CVE-2019-6163 CONFIRM
linux -- linux_kernel	A NULL pointer dereference vulnerability in the function nfc_genl_deactivate_target() in net/nfc/netlink.c in the Linux kernel before 5.1.13 can be triggered by a malicious user-mode program that omits certain NFC attributes, leading to denial of service.	2019-06-26	4.3	CVE-2019-12984 BID MISC MISC
livezilla -- livezilla	LiveZilla Server before 8.0.1.1 is vulnerable to CSV Injection in the Export Function.	2019-06-25	6.8	CVE-2019-12961 MISC
livezilla -- livezilla	LiveZilla Server before 8.0.1.1 is vulnerable to XSS in mobile/index.php via the Accept-Language HTTP header.	2019-06-25	4.3	CVE-2019-12962 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
livezilla -- livezilla	LiveZilla Server before 8.0.1.1 is vulnerable to XSS in the chat.php Create Ticket Action.	2019-06-25	4.3	CVE-2019-12963 MISC
livezilla -- livezilla	LiveZilla Server before 8.0.1.1 is vulnerable to XSS in the ticket.php Subject.	2019-06-25	4.3	CVE-2019-12964 MISC
moodle -- moodle	A flaw was found in Moodle before 3.7, 3.6.4, 3.5.6, 3.4.9 and 3.1.18. The form to upload cohorts contained a redirect field, which was not restricted to internal URLs.	2019-06-26	5.8	CVE-2019-10133 CONFIRM CONFIRM
moodle -- moodle	A flaw was found in Moodle before 3.7, 3.6.4, 3.5.6, 3.4.9 and 3.1.18. The size of users' private file uploads via email were not correctly checked, so their quota allowance could be exceeded.	2019-06-26	4.3	CVE-2019-10134 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
moodle -- moodle	A flaw was found in Moodle before versions 3.7, 3.6.4. A web service fetching messages was not restricted to the current user's conversations.	2019-06-26	5.0	CVE-2019-10154 CONFIRM CONFIRM
netgate -- pfsense	In pfSense 2.4.4-p2 and 2.4.4-p3, if it is possible to trick an authenticated administrator into clicking on a button on a phishing page, an attacker can leverage XSS to upload arbitrary executable code, via diag_command.php and rrd_fetch_json.php (timePeriod parameter), to a server. Then, the remote attacker can run any command with root privileges on that server.	2019-06-25	4.3	CVE-2019-12949 MISC
netiq -- self_service_password_reset	A potential XSS exists in Self Service Password Reset, in Micro Focus NetIQ	2019-06-24	4.3	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Software all versions prior to version 4.4. The vulnerability could be exploited to enable an XSS attack.			11647 CONFIRM
netiq -- self_service_password_reset	An information leakage exists in Micro Focus NetIQ Self Service Password Reset Software all versions prior to version 4.4. The vulnerability could be exploited to expose sensitive information.	2019-06-24	5.0	CVE-2019-11648 CONFIRM
openjpeg -- openjpeg	Division-by-zero vulnerabilities in the functions pi_next_pcrl, pi_next_cprl, and pi_next_rpcl in openmj2/pi.c in OpenJPEG through 2.3.0 allow remote attackers to cause a denial of service (application crash).	2019-06-26	4.3	CVE-2018-20845 BID MISC
openjpeg -- openjpeg	Out-of-bounds accesses in the functions pi_next_lrcp, pi_next_rlcp, pi_next_rpcl, pi_next_pcrl, pi_next_rpcl, and pi_next_cprl in openmj2/pi.c in OpenJPEG through 2.3.0 allow remote attackers to cause a denial of service (application crash).	2019-06-26	4.3	CVE-2018-20846 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openjpeg -- openjpeg	An improper computation of p_tx0, p_tx1, p_ty0 and p_ty1 in the function opj_get_encoding_parameters in openjp2/pi.c in OpenJPEG through 2.3.0 can lead to an integer overflow.	2019-06-26	6.8	CVE-2018-20847 BID MISC MISC MISC
openjpeg -- openjpeg	In OpenJPEG 2.3.1, there is excessive iteration in the opj_t1_encode_cblks function of openjp2/t1.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file. This issue is similar to CVE-2018-6616.	2019-06-26	4.3	CVE-2019-12973 BID MISC MISC
phoenixcontact -- automationworx_software_suite	An issue was discovered in PHOENIX CONTACT PC Worx through 1.86, PC Worx Express through 1.86, and Config+ through 1.86. A manipulated PC Worx or Config+ project file could lead to an Out-Of-Bounds Read, Information Disclosure, and remote code execution. The attacker needs to get access to an original PC Worx or Config+ project file to be able to	2019-06-24	6.8	CVE-2019-12869 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	manipulate it. After manipulation, the attacker needs to exchange the original file with the manipulated one on the application programming workstation.			
phoenixcontact -- automationworx_software_suite	An issue was discovered in PHOENIX CONTACT PC Worx through 1.86, PC Worx Express through 1.86, and Config+ through 1.86. A manipulated PC Worx or Config+ project file could lead to an Uninitialized Pointer and remote code execution. The attacker needs to get access to an original PC Worx or Config+ project file to be able to manipulate it. After manipulation, the attacker needs to exchange the original file with the manipulated one on the application programming workstation.	2019-06-24	6.8	CVE-2019-12870 MISC MISC
phoenixcontact -- automationworx_software_suite	An issue was discovered in PHOENIX CONTACT PC Worx through 1.86, PC Worx Express through 1.86, and Config+ through 1.86. A manipulated PC Worx or Config+ project file could lead to a Use-After-Free and remote code execution.	2019-06-24	6.8	CVE-2019-12871 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The attacker needs to get access to an original PC Worx or Config+ project file to be able to manipulate it. After manipulation, the attacker needs to exchange the original file with the manipulated one on the application programming workstation.			
shopware -- shopware	Shopware before 5.5.8 has XSS via the Query String to the backend/Login or backend/Login/load/ URI.	2019-06-23	4.3	CVE-2019-12935 MISC FULLDISC MISC MISC
tenable -- nessus	Nessus versions 8.4.0 and earlier were found to contain a reflected XSS vulnerability due to improper validation of user-supplied input. An unauthenticated, remote attacker could potentially exploit this vulnerability via a specially crafted request to execute	2019-06-25	4.3	CVE-2019-3961 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary script code in a users browser session.			
ultimatemember -- ultimate_member	An issue was discovered in the Ultimate Member plugin 2.39 for WordPress. It allows unauthorized profile and cover picture modification. It is possible to modify the profile and cover picture of any user once one is connected. One can also modify the profiles and cover pictures of privileged users. To perform such a modification, one first needs to (for example) intercept an upload-picture request and modify the user_id parameter.	2019-06-24	4.0	CVE-2019-10271 MISC
zyxel -- uag2100_firmware	A reflective Cross-site scripting (XSS) vulnerability in the free_time_failed.cgi CGI program in selected Zyxel ZyWall, USG, and UAG devices allows remote attackers to inject arbitrary web script or HTML via the err_msg parameter.	2019-06-27	4.3	CVE-2019-12581 MISC MISC CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zyxel -- uag2100_firmware	Missing Access Control in the "Free Time" component of several Zyxel UAG, USG, and ZyWall devices allows a remote attacker to generate guest accounts by directly accessing the account generator. This can lead to unauthorised network access or Denial of Service.	2019-06-27	6.4	CVE-2019-12583 MISC CONFIRM

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Use of extended attributes in downloads in Google Chrome prior to 72.0.3626.81 allowed a local attacker to read download URLs via the filesystem.	2019-06-27	2.1	CVE-2018-20073 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- pureapplication_system	IBM PureApplication System 2.2.3.0 through 2.2.5.3 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 159242.	2019-06-26	2.1	CVE-2019-4225 XF CONFIRM
ibm -- rational_collaborative_lifecycle_management	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 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: 148605.	2019-06-27	3.5	CVE-2018-1758 CONFIRM XF
ibm -- rational_collaborative_lifecycle_management	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 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	2019-06-27	3.5	CVE-2018-1760 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disclosure within a trusted session. IBM X-Force ID: 148614.			
ibm -- rational_collaborative_lifecycle_management	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 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: 150429.	2019-06-27	3.5	CVE-2018-1826 CONFIRM XF
ibm -- rational_collaborative_lifecycle_management	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 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: 150430.	2019-06-27	3.5	CVE-2018-1827 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- rational_collaborative_lifecycle_management	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 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: 150431.	2019-06-27	3.5	CVE-2018-1828 CONFIRM XF
ibm -- rational_collaborative_lifecycle_management	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 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: 152156.	2019-06-27	3.5	CVE-2018-1892 CONFIRM XF
ibm -- rational_collaborative_lifecycle_management	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript	2019-06-27	3.5	CVE-2018-1893 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152157.			
ibm -- rational_collaborative_lifecycle_management	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) 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: 157383.	2019-06-27	3.5	CVE-2019-4083 CONFIRM XF
ibm -- rational_collaborative_lifecycle_management	IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1 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	2019-06-27	3.5	CVE-2019-4249 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disclosure within a trusted session. IBM X-Force ID: 159647.			
ibm -- rational_collaborative_lifecycle_management	IBM Jazz Foundation products (IBM Rational Collaborative Lifecycle Management 6.0 through 6.0.6.1) 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: 159648.	2019-06-27	3.5	CVE-2019-4250 CONFIRM XF
ibm -- security_access_manager	IBM Security Access Manager 9.0.1 through 9.0.6 could reveal highly sensitive in specialized conditions to a local user which could be used in further attacks against the system. IBM X-Force ID: 158400.	2019-06-25	3.6	CVE-2019-4145 XF CONFIRM
ibm -- security_access_manager	IBM Security Access Manager 9.0.1 through 9.0.6 does not invalidate session tokens in a timely	2019-06-25	3.6	CVE-2019-4152

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	manner. The lack of proper session expiration may allow attackers with local access to login into a closed browser session. IBM X-Force ID: 158515.			XF CONFIRM
ibm -- security_access_manager	IBM Security Access Manager 9.0.1 through 9.0.6 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 158517.	2019-06-25	3.5	CVE-2019-4153 XF CONFIRM
polycom -- better_together_over_ethernet_connector	VVX products using UCS software version 5.9.2 and earlier with Better Together over Ethernet Connector (BToE) application version 3.9.1 and earlier provides insufficient	2019-06-24	3.3	CVE-2019-10689 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authentication between the BToE application and the BToE component, resulting in leakage of sensitive information.			
quadbase -- espressreport_es	Stored XSS within Quadbase EspressReport ES (ERES) v7.0 update 7 allows remote attackers to execute malicious JavaScript and inject arbitrary source code into the target pages. The XSS payload is stored by creating a new user account, and setting the username to an XSS payload. The stored payload can then be triggered by accessing the "Set Security Levels" or "View User/Group Relationships" page. If the attacker does not currently have permission to create a new user, another vulnerability such as CSRF must be exploited first.	2019-06-24	3.5	CVE-2019-9957 MISC
redhat -- cloudforms_management_engine	A stored cross-site scripting (XSS) vulnerability was found in the PDF export component of CloudForms, versions 5.9 and 5.10, due to user	2019-06-27	3.5	CVE-2019-10177 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	input is not properly sanitized. An attacker with least privilege to edit compute is able to execute a XSS attack against other users, which could lead to malicious code execution and extraction of the anti-CSRF token of higher privileged users.			

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- cp635_hmi	The ABB CP635 HMI uses two different transmission methods to upgrade its firmware and its software components: "Utilization of USB/SD Card to flash the device" and "Remote provisioning process via ABB Panel Builder 600 over FTP." Neither of these transmission methods implements any form of encryption or authenticity checks against the new firmware HMI software binary files.	2019-06-24	not yet calculated	CVE-2019-7229 MISC MISC CONFIRM CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				RM MISC
abb -- hmi_components	The ABB HMI components implement hidden administrative accounts that are used during the provisioning phase of the HMI interface. These credentials allow the provisioning tool "Panel Builder 600" to flash a new interface and Tags (MODBUS coils) mapping to the HMI. These credentials are the idal123 password for the IdalMaster account, and the exor password for the exor account. These credentials are used over both HTTP(S) and FTP. There is no option to disable or change these undocumented credentials. An attacker can use these credentials to login to ABB HMI to read/write HMI configuration files and also to reset the device. This affects ABB CP635 HMI, CP600 HMIClient, Panel Builder 600, IDAL FTP server, IDAL HTTP server, and multiple other HMI components.	2019-06-27	not yet calculated	CVE-2019-7225 MISC FULLDISC BID MISC
abb -- idal_ftp_server	The ABB IDAL FTP server is vulnerable to a buffer overflow when a long string is sent by an authenticated attacker. This overflow is handled, but terminates the process. An	2019-06-24	not yet calculated	CVE-2019-7231 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated attacker can send a FTP command string of 472 bytes or more to overflow a buffer, causing an exception that terminates the server.			FULLDISC BID CONFIRM MISC
abb -- idal_ftp_server	The ABB IDAL FTP server mishandles format strings in a username during the authentication process. Attempting to authenticate with the username %s%p%x%d will crash the server. Sending %08x.AAAA.%08x.%08x will log memory content from the stack.	2019-06-24	not yet calculated	CVE-2019-7230 MISC MISC BID CONFIRM MISC
abb -- idal_ftp_server	In the ABB IDAL FTP server, an authenticated attacker can traverse to arbitrary directories on the hard disk with "CWD ../" and then use the FTP server functionality to download and upload files. An unauthenticated attacker can take advantage of the hardcoded or default credential pair exor/exor to become an authenticated attacker.	2019-06-27	not yet calculated	CVE-2019-7227 MISC FULLDISC BID CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				RM MISC
abb -- idal_http_server	The ABB IDAL HTTP server mishandles format strings in a username or cookie during the authentication process. Attempting to authenticate with the username %25s%25p%25x%25n will crash the server. Sending %08x.AAAA.%08x.%08x will log memory content from the stack.	2019-06-27	not yet calculated	CVE-2019-7228 MISC FULLDISC BID CONFIRM MISC
abb -- idal_http_server	The ABB IDAL HTTP server is vulnerable to a buffer overflow when a long Host header is sent in a web request. The Host header value overflows a buffer and overwrites a Structured Exception Handler (SEH) address. An unauthenticated attacker can submit a Host header value of 2047 bytes or more to overflow the buffer and overwrite the SEH address, which can then be leveraged to execute attacker-controlled code on the server.	2019-06-24	not yet calculated	CVE-2019-7232 MISC MISC BID CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- idal_http_server	The ABB IDAL HTTP server CGI interface contains a URL that allows an unauthenticated attacker to bypass authentication and gain access to privileged functions. Specifically, /cgi/loginDefaultUser creates a session in an authenticated state and returns the session ID along with what may be the username and cleartext password of the user. An attacker can then supply an IDALToken value in a cookie, which will allow them to perform privileged operations such as restarting the service with /cgi/restart. A GET request to /cgi/loginDefaultUser may result in "1 #S_OK IDALToken=532c8632b86694f0232a68a0897a145c admin admin" or a similar response.	2019-06-27	not yet calculated	CVE-2019-7226 MISC FULLDISC BID MISC
actiontec -- web6000q_devices	An issue was discovered in the Quantenna WiFi Controller on Telus Actiontec WEB6000Q v1.1.02.22 devices. An attacker can statically set his/her IP to anything on the 169.254.1.0/24 subnet, and obtain root access by connecting to 169.254.1.2 port 23 with telnet/netcat.	2019-06-27	not yet calculated	CVE-2018-15557 MISC FULLDISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
actiontec -- web6000q_devices	The Quantenna WiFi Controller on Telus Actiontec WEB6000Q v1.1.02.22 allows login with root level access with the user "root" and an empty password by using the enabled onboard UART headers.	2019-06-27	not yet calculated	CVE-2018-15556 MISC MISC
actiontec -- web6000q_devices	On Telus Actiontec WEB6000Q v1.1.02.22 devices, an attacker can login with root level access with the user "root" and password "admin" by using the enabled onboard UART headers.	2019-06-28	not yet calculated	CVE-2018-15555 MISC FULLDISC
advanced_micro_devices -- platform_security_processor	Secure Encrypted Virtualization (SEV) on Advanced Micro Devices (AMD) Platform Security Processor (PSP; aka AMD Secure Processor or AMD-SP) 0.17 build 11 and earlier has an insecure cryptographic implementation.	2019-06-25	not yet calculated	CVE-2019-9836 MISC MISC CONFIRM
advantech -- webaccess/scada	In WebAccess/SCADA, Versions 8.3.5 and prior, a path traversal vulnerability is caused by a lack of proper validation of a user-supplied path prior to use in file operations. An	2019-06-28	not yet calculated	CVE-2019-10985 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker can leverage this vulnerability to delete files while posing as an administrator.			
advantech -- webaccess/scada	In WebAccess/SCADA Versions 8.3.5 and prior, an out-of-bounds read vulnerability is caused by a lack of proper validation of user-supplied data. Exploitation of this vulnerability may allow disclosure of information.	2019-06-28	not yet calculated	CVE-2019-10983 MISC
advantech -- webaccess/scada	In WebAccess/SCADA Versions 8.3.5 and prior, multiple heap-based buffer overflow vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution. Note: A different vulnerability than CVE-2019-10991.	2019-06-28	not yet calculated	CVE-2019-10989 MISC
advantech -- webaccess/scada	In WebAccess/SCADA Versions 8.3.5 and prior, multiple out-of-bounds write vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution.	2019-06-28	not yet calculated	CVE-2019-10987 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
advantech -- webaccess/scada	In WebAccess/SCADA Versions 8.3.5 and prior, multiple untrusted pointer dereference vulnerabilities may allow a remote attacker to execute arbitrary code.	2019-06-28	not yet calculated	CVE-2019-10993 MISC
advantech -- webaccess/scada	In WebAccess/SCADA, Versions 8.3.5 and prior, multiple stack-based buffer overflow vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution.	2019-06-28	not yet calculated	CVE-2019-10991 MISC
asus -- hivivo_application	The ASUS HiVivo application before 5.6.27 for ASUS Watch has Missing SSL Certificate Validation.	2019-06-24	not yet calculated	CVE-2017-17945 MISC
bluestacks -- app_player	BlueStacks App Player 2, 3, and 4 before 4.90 allows DNS Rebinding for attacks on exposed IPC functions.	2019-06-23	not yet calculated	CVE-2019-12936 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
couchbase -- couchbase_sync_gateway_and_couchbase_server	The Couchbase Sync Gateway 2.1.2 in combination with a Couchbase Server is affected by a previously undisclosed N1QL-injection vulnerability in the REST API. An attacker with access to the public REST API can insert additional N1QL statements through the parameters ?startkey? and ?endkey? of the ?_all_docs? endpoint.	2019-06-26	not yet calculated	CVE-2019-9039 CONFIRM MISC
diffplug -- spotless	In DiffPlug Spotless before 1.20.0 (library and Maven plugin) and before 3.20.0 (Gradle plugin), the XML parser would resolve external entities over both HTTP and HTTPS and didn't respect the resolveExternalEntities setting. For example, this allows disclosure of file contents to a MITM attacker if a victim performs a spotlessApply operation on an untrusted XML file.	2019-06-28	not yet calculated	CVE-2019-9843 MISC MISC MISC MISC
digitaldruid -- hoteldruid	Hoteldruid before v2.3.1 allows remote authenticated users to cause a denial of service (invoice-creation outage) via the n_file parameter to visualizza_contratto.php with invalid arguments (any non-numeric value), as demonstrated by the anno=2019&id_transazione=1&numero_contr	2019-06-24	not yet calculated	CVE-2019-9085 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	atto=1&n_file=a query string to visualizza_contratto.php.			
doomseeker -- doomseeker	A vulnerability was found in the Sonic Robo Blast 2 (SRB2) plugin (EP_Versions 9 to 11 inclusive) distributed with Doomseeker 1.1 and 1.2. Affected plugin versions did not discard IP packets with an unnaturally long response length from a Sonic Robo Blast 2 master server, allowing a remote attacker to cause a potential crash / denial of service in Doomseeker. The issue has been remediated in the Doomseeker 1.3 release with source code patches to the SRB2 plugin.	2019-06-26	not yet calculated	CVE-2019-12968 MISC MISC MISC MISC
facebook_open_source -- hhvm	HHVM, when used with FastCGI, would bind by default to all available interfaces. This behavior could allow a malicious individual unintended direct access to the application, which could result in information disclosure. This issue affects versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.7.0, 4.8.0, versions 3.30.5 and below, and all versions in the 4.0, 4.1, and 4.2 series.	2019-06-26	not yet calculated	CVE-2019-3569 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fehelper -- fehelper	FeHelper through 2019-06-19 allows arbitrary code execution during a JSON format operation, as demonstrated by the {"a":(function(){confirm(1)})()} input.	2019-06-26	not yet calculated	CVE-2019-12966 MISC
flightcrew -- flightcrew	An issue was discovered in FlightCrew v0.9.2 and earlier. A NULL pointer dereference occurs in GetRelativePathToNcx() or GetRelativePathsToXhtmlDocuments() when a NULL pointer is passed to xc::XMLUri::isValidURI(). This affects third-party software (not Sigil) that uses FlightCrew as a library.	2019-06-28	not yet calculated	CVE-2019-13032 MISC
gnome -- glib	The keyfile settings backend in GNOME GLib (aka glib2.0) before 2.59.1 creates directories using g_file_make_directory_with_parents (kfsb->dir, NULL, NULL) and files using g_file_replace_contents (kfsb->file, contents, length, NULL, FALSE, G_FILE_CREATE_REPLACE_DESTINATION, NULL, NULL, NULL). Consequently, it does not properly restrict directory (and file) permissions. Instead, for directories, 0777 permissions are used; for files, default file	2019-06-28	not yet calculated	CVE-2019-13012 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	permissions are used. This is similar to CVE-2019-12450.			
google -- chrome	Incorrect convexity calculations in Skia in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5785 MISC MISC
google -- chrome	Integer overflow in download manager in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5829 SUSE MISC MISC FEDORA
google -- chrome	Insufficient file type enforcement in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to obtain local file data via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2018-16075 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Type confusion in WebRTC in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.	2019-06-27	not yet calculated	CVE-2018-6157 MISC MISC
google -- chrome	Insufficient policy enforcement in ServiceWorker in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2018-6159 MISC MISC
google -- chrome	Type confusion in JavaScript in Google Chrome prior to 67.0.3396.87 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2018-6149 MISC MISC
google -- chrome	Incorrect implementation in Content Security Policy in Google Chrome prior to 67.0.3396.79 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2018-6148 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Insufficient data validation in HTML parser in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to bypass same origin policy via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2018-6145 MISC MISC
google -- chrome	Use after free in Bluetooth in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension.	2019-06-27	not yet calculated	CVE-2018-6171 MISC MISC
google -- chrome	Incorrect handling of object lifetimes in WebRTC in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2018-6130 MISC MISC
google -- chrome	Object lifecycle issue in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2018-16077 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Object lifecycle issue in ServiceWorker in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5828 SUSE MISC MISC FEDORA
google -- chrome	Object lifetime issue in Blink in Google Chrome prior to 72.0.3626.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5786 MISC MISC
google -- chrome	Incorrect handling of CORS in ServiceWorker in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2018-6150 MISC MISC
google -- chrome	Out of bounds array access in WebRTC in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially perform out of	2019-06-27	not yet calculated	CVE-2018-6129

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bounds memory access via a crafted HTML page.			MISC MISC
google -- chrome	Insufficient policy enforcement in site isolation in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass site isolation via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2018-16074 MISC MISC
google -- chrome	Object lifecycle issue in V8 in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5831 SUSE MISC MISC FEDORA
google -- chrome	Incorrect URL parsing in WebKit in Google Chrome on iOS prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2018-6128 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Insufficient validation of input in Blink in Google Chrome prior to 66.0.3359.170 allowed a remote attacker to perform privilege escalation via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2018-6121 MISC MISC
google -- chrome	Integer overflows in Skia in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2018-16070 MISC MISC
google -- chrome	Insufficient policy enforcement in extensions API in Google Chrome prior to 69.0.3497.81 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.	2019-06-27	not yet calculated	CVE-2018-16086 MISC MISC
google -- chrome	Incorrect handling of frames in the VP8 parser in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.	2019-06-27	not yet calculated	CVE-2018-6155 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Parameter passing error in media in Google Chrome prior to 74.0.3729.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5824 SUSE MISC MISC FEDORA
google -- chrome	Insufficient policy enforcement in site isolation in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass site isolation via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2018-16073 MISC MISC
google -- chrome	Incorrect handling of deferred code in V8 in Google Chrome prior to 72.0.3626.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5784 MISC MISC
google -- chrome	Integer overflow in PDFium in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2019-06-27	not yet calculated	CVE-2019-5820 SUSE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC FEDORA
google -- chrome	Resource size information leakage in Blink in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5837 SUSE MISC MISC FEDORA
google -- chrome	Insufficient data validation in developer tools in Google Chrome on OS X prior to 74.0.3729.108 allowed a local attacker to execute arbitrary code via a crafted string copied to clipboard.	2019-06-27	not yet calculated	CVE-2019-5819 SUSE MISC MISC FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Insufficient policy enforcement in XMLHttpRequest in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5832 SUSE MISC MISC FEDORA
google -- chrome	Use-after-free in PDFium in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2019-06-27	not yet calculated	CVE-2019-5805 SUSE MISC MISC FEDORA
google -- chrome	Insufficient policy enforcement in extensions API in Google Chrome prior to 75.0.3770.80 allowed an attacker who convinced a user to install a malicious extension to bypass restrictions on file URIs via a crafted Chrome Extension.	2019-06-27	not yet calculated	CVE-2019-5838 SUSE MISC MISC FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Incorrect dialog box scoping in browser in Google Chrome on Android prior to 75.0.3770.80 allowed a remote attacker to display misleading security UI via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5833 SUSE MISC MISC FEDORA
google -- chrome	Insufficient policy enforcement in service workers in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5823 SUSE MISC MISC
google -- chrome	Insufficient data validation in Blink in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5834 SUSE MISC MISC FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Inappropriate implementation in Blink in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass same origin policy via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5822 SUSE MISC MISC FEDORA
google -- chrome	Integer overflow in PDFium in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2019-06-27	not yet calculated	CVE-2019-5821 SUSE MISC MISC FEDORA
google -- chrome	Integer overflow in SQLite via WebSQL in Google Chrome prior to 74.0.3729.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5827 SUSE MISC MISC FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Object lifecycle issue in SwiftShader in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5835 SUSE MISC MISC FEDORA
google -- chrome	Integer overflow in ANGLE in Google Chrome on Windows prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5806 SUSE MISC MISC FEDORA
google -- chrome	Insufficient policy enforcement in CORS in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5830 SUSE MISC MISC FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Heap buffer overflow in ANGLE in Google Chrome on Windows prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5817 SUSE MISC MISC
google -- chrome	Process lifetime issue in Chrome in Google Chrome on Android prior to 74.0.3729.108 allowed a remote attacker to potentially persist an exploited process via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5816 SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in Blink in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5814 SUSE MISC MISC FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Excessive data validation in URL parser in Google Chrome prior to 75.0.3770.80 allowed a remote attacker who convinced a user to input a URL to bypass website URL validation via a crafted URL.	2019-06-27	not yet calculated	CVE-2019-5839 SUSE MISC MISC FEDORA
google -- chrome	Heap buffer overflow in ANGLE in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5836 SUSE MISC MISC FEDORA
google -- chrome	Inadequate security UI in iOS UI in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5812 SUSE MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Incorrect handling of CORS in ServiceWorker in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass same origin policy via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5811 SUSE MISC MISC FEDORA
google -- chrome	Object lifetime issue in V8 in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-06-27	not yet calculated	CVE-2019-5807 SUSE MISC MISC FEDORA
google -- chrome	Uninitialized data in media in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted video file.	2019-06-27	not yet calculated	CVE-2019-5818 SUSE MISC MISC FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
grafana -- grafana	public/app/features/panel/panel_ctrl.ts in Grafana before 6.2.5 allows HTML Injection in panel drilldown links (via the Title or url field).	2019-06-29	not yet calculated	CVE-2019-13068 MISC MISC
grouptime -- teamwire_desktop_client	The admin interface of the Grouptime Teamwire Desktop Client 1.5.1 prior to 1.9.0 on-premises messenger server allows stored XSS. All backend versions prior to prod-2018-11-13-15-00-42 are affected.	2019-06-28	not yet calculated	CVE-2018-17560 MISC
grouptime -- teamwire_desktop_client	Grouptime Teamwire Desktop Client 1.5.1 prior to 1.9.0 on Windows allows code injection via a template, leading to remote code execution. All backend versions prior to prod-2018-11-13-15-00-42 are affected.	2019-06-28	not yet calculated	CVE-2018-17170 MISC
hosting_controller -- hc10_hc.server_service	The HC.Server service in Hosting Controller HC10 10.14 allows an Invalid Pointer Write DoS.	2019-06-24	not yet calculated	CVE-2019-12323 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- bigfix_inventory	IBM BigFix Inventory v9 (SUA v9 / ILMT v9) discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 161807.	2019-06-28	not yet calculated	CVE-2019-4369 CONFIRM XF
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Admin Console could allow a remote attacker to obtain sensitive information when a specially crafted url causes a stack trace to be dumped. IBM X-Force ID: 160202.	2019-06-28	not yet calculated	CVE-2019-4269 XF CONFIRM
icon_project -- loopchain	In Loopchain through 2.2.1.3, an attacker can escalate privileges from a low-privilege shell by changing the environment (aka injection in the DEFAULT_SCORE_HOST environment variable).	2019-06-28	not yet calculated	CVE-2019-12997 MISC
irssi -- irssi	Irssi before 1.0.8, 1.1.x before 1.1.3, and 1.2.x before 1.2.1, when SASL is enabled, has a use after free when sending SASL login to the server.	2019-06-29	not yet calculated	CVE-2019-13045 MLIST MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC BUGTRAQ
istio -- istio	Istio before 1.2.2 mishandles certain access tokens, leading to "Epoch 0 terminated with an error" in Envoy. This is related to a jwt_authenticator.cc segmentation fault.	2019-06-28	not yet calculated	CVE-2019-12995 MISC MISC MISC
keyidentity -- linotp	KeyIdentity LinOTP before 2.10.5.3 has Incorrect Access Control (issue 1 of 2).	2019-06-27	not yet calculated	CVE-2019-12887 MISC
lemonldap-ng -- lemonldap-ng	LemonLDAP::NG before 1.9.20 has an XML External Entity (XXE) issue when submitting a notification to the notification server. By default, the notification server is not enabled and has a "deny all" rule.	2019-06-28	not yet calculated	CVE-2019-13031 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lenovo -- service_bridge	A vulnerability reported in Lenovo Service Bridge before version 4.1.0.1 could allow cross-site request forgery.	2019-06-26	not yet calculated	CVE-2019-6166 CONFIRM
lenovo -- service_bridge	A vulnerability reported in Lenovo Service Bridge before version 4.1.0.1 could allow remote code execution.	2019-06-26	not yet calculated	CVE-2019-6167 CONFIRM
lenovo -- service_bridge	A vulnerability reported in Lenovo Service Bridge before version 4.1.0.1 could allow unencrypted downloads over FTP.	2019-06-26	not yet calculated	CVE-2019-6169 CONFIRM
lenovo -- service_bridge	A vulnerability reported in Lenovo Service Bridge before version 4.1.0.1 could allow remote code execution.	2019-06-26	not yet calculated	CVE-2019-6168 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lexmark -- multiple_devices	Various Lexmark devices have a Buffer Overflow (issue 2 of 2).	2019-06-28	not yet calculated	CVE-2018-15520 CONFIRM
lexmark -- multiple_devices	Various Lexmark devices have a Buffer Overflow (issue 1 of 2).	2019-06-28	not yet calculated	CVE-2018-15519 CONFIRM
libming -- libming	Ming (aka libming) 0.4.8 has a heap buffer overflow and underflow in the decompileCAST function in util/decompile.c in libutil.a. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted SWF file.	2019-06-26	not yet calculated	CVE-2019-12982 MISC
libming -- libming	In Ming (aka libming) 0.4.8, there is an integer overflow (caused by an out-of-range left shift) in the SWFInput_readSBits function in blocks/input.c. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted swf file.	2019-06-26	not yet calculated	CVE-2019-12980 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
libming -- libming	Ming (aka libming) 0.4.8 has an "fill overflow" vulnerability in the function SWFShape_setLeftFillStyle in blocks/shape.c.	2019-06-26	not yet calculated	CVE-2019-12981 MISC
logitech -- r500_presentation_clicker	The Logitech R500 presentation clicker allows attackers to determine the AES key, leading to keystroke injection. On Windows, any text may be injected by using ALT+NUMPAD input to bypass the restriction on the characters A through Z.	2019-06-29	not yet calculated	CVE-2019-13054 MISC
logitech -- unifying_devices	Logitech Unifying devices before 2016-02-26 allow keystroke injection, bypassing encryption, aka MouseJack.	2019-06-29	not yet calculated	CVE-2016-10761 MISC MISC
logitech -- unifying_devices	Logitech Unifying devices allow live decryption if the pairing of a keyboard to a receiver is sniffed.	2019-06-29	not yet calculated	CVE-2019-13052 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
logitech -- unifying_devices	Certain Logitech Unifying devices allow attackers to dump AES keys and addresses, leading to the capability of live decryption of Radio Frequency transmissions, as demonstrated by an attack against a Logitech K360 keyboard.	2019-06-29	not yet calculated	CVE-2019-13055 MISC
logitech -- unifying_devices	Logitech Unifying devices allow keystroke injection, bypassing encryption. The attacker must press a "magic" key combination while sniffing cryptographic data from a Radio Frequency transmission. NOTE: this issue exists because of an incomplete fix for CVE-2016-10761.	2019-06-29	not yet calculated	CVE-2019-13053 MISC
loytec -- lgate-902_devices	LOYTEC LGATE-902 6.3.2 devices allow Arbitrary file deletion.	2019-06-28	not yet calculated	CVE-2018-14916 MISC FULLDISC FULLDISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
loytec -- lgate-902_devices	LOYTEC LGATE-902 6.3.2 devices allow Directory Traversal.	2019-06-28	not yet calculated	CVE-2018-14918 MISC FULLDISC FULLDISC
loytec -- lgate-902_devices	LOYTEC LGATE-902 6.3.2 devices allow XSS.	2019-06-28	not yet calculated	CVE-2018-14919 MISC FULLDISC FULLDISC MISC
makerbot -- replicator_5g_printer	The MakerBot Replicator 5G printer runs an Apache HTTP Server with directory indexing enabled. Apache logs, system logs, design files (i.e., a history of print files), and more are exposed to unauthenticated attackers through this HTTP server.	2019-06-24	not yet calculated	CVE-2014-9699 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mcafee -- enterprise_security_manager	Directory Traversal vulnerability in McAfee Enterprise Security Manager (ESM) prior to 11.2.0 and prior to 10.4.0 allows authenticated user to gain elevated privileges via specially crafted input.	2019-06-27	not yet calculated	CVE-2019-3632 CONFIRM
mcafee -- enterprise_security_manager	Privilege escalation in McAfee Enterprise Security Manager (ESM) 11.x prior to 11.2.0 allows authenticated user to gain access to a core system component via incorrect access control.	2019-06-27	not yet calculated	CVE-2019-3628 CONFIRM
mcafee -- enterprise_security_manager	Application protection bypass vulnerability in McAfee Enterprise Security Manager (ESM) prior to 11.2.0 and prior to 10.4.0 allows unauthenticated user to impersonate system users via specially crafted parameters.	2019-06-27	not yet calculated	CVE-2019-3629 CONFIRM
mcafee -- enterprise_security_manager	Command Injection vulnerability in McAfee Enterprise Security Manager (ESM) prior to 11.2.0 and prior to 10.4.0 allows authenticated user to execute arbitrary code via specially crafted parameters.	2019-06-27	not yet calculated	CVE-2019-3630 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mcafee -- enterprise_security_manager	Command Injection vulnerability in McAfee Enterprise Security Manager (ESM) prior to 11.2.0 and prior to 10.4.0 allows authenticated user to execute arbitrary code via specially crafted parameters.	2019-06-27	not yet calculated	CVE-2019-3631 CONFIRM
medtronic -- minimed_508_and_paradigm_series_insulin_pumps	In Medtronic MinMed 508 and Medtronic Minimed Paradigm Insulin Pumps, Versions, MiniMed 508 pump ? All versions, MiniMed Paradigm 511 pump ? All versions, MiniMed Paradigm 512/712 pumps ? All versions, MiniMed Paradigm 712E pump?All versions, MiniMed Paradigm 515/715 pumps?All versions, MiniMed Paradigm 522/722 pumps ? All versions,MiniMed Paradigm 522K/722K pumps ? All versions, MiniMed Paradigm 523/723 pumps ? Software versions 2.4A or lower, MiniMed Paradigm 523K/723K pumps ? Software, versions 2.4A or lower, MiniMed Paradigm Veo 554/754 pumps ? Software versions 2.6A or lower, MiniMed Paradigm Veo 554CM and 754CM models only ? Software versions 2.7A or lower, the affected insulin pumps are designed to communicate using a wireless RF with other devices, such as blood glucose meters, glucose sensor	2019-06-28	not yet calculated	CVE-2019-10964 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	transmitters, and CareLink USB devices. This wireless RF communication protocol does not properly implement authentication or authorization. An attacker with adjacent access to one of the affected insulin pump models can inject, replay, modify, and/or intercept data. This vulnerability could also allow attackers to change pump settings and control insulin delivery.			
ministry_of_interior_of_the_slovak_republic -- eid_client	An incorrect implementation of a local web server in eID client (Windows version before 3.1.2, Linux version before 3.0.3) allows remote attackers to execute arbitrary code (.cgi, .pl, or .php) or delete arbitrary files via a crafted HTML page. This is a product from the Ministry of Interior of the Slovak Republic.	2019-06-28	not yet calculated	CVE-2019-13028 MISC MISC MISC
nginx -- nginx	njs through 0.3.3, used in NGINX, has a buffer over-read in nxt_utf8_decode in nxt/nxt_utf8.c. This issue occurs after the fix for CVE-2019-12207 is in place.	2019-06-29	not yet calculated	CVE-2019-13067 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
odoo -- community_and_enterprise	Incorrect access control in the database manager component in Odoo Community 10.0 and 11.0 and Odoo Enterprise 10.0 and 11.0 allows a remote attacker to restore a database dump without knowing the super-admin password. An arbitrary password succeeds.	2019-06-28	not yet calculated	CVE-2018-14885 MISC CONFIRM
odoo -- community_and_enterprise	Incorrect access control in the portal messaging system in Odoo Community 9.0 and 10.0 and Odoo Enterprise 9.0 and 10.0 allows remote attackers to post messages on behalf of customers, and to guess document attribute values, via crafted parameters.	2019-06-28	not yet calculated	CVE-2018-14867 MISC CONFIRM
odoo -- community_and_enterprise	Incorrect access control in the Password Encryption module in Odoo Community 9.0 and Odoo Enterprise 9.0 allows authenticated users to change the password of other users without knowing their current password via a crafted RPC call.	2019-06-28	not yet calculated	CVE-2018-14868 MISC CONFIRM
odoo -- community_and_enterprise	The module-description renderer in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier does not disable RST's local file inclusion, which allows	2019-06-28	not yet calculated	CVE-2018-14886 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privileged authenticated users to read local files via a crafted module description.			CONFIRM
odoo -- community_and_enterprise	Improper Host header sanitization in the dbfilter routing component in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows a remote attacker to deny access to the service and to disclose database names via a crafted request.	2019-06-28	not yet calculated	CVE-2018-14887 MISC CONFIRM
pandora_fms -- pandora_fms	Artica Pandora FMS 7.0 NG before 735 suffers from local privilege escalation due to improper permissions on C:\PandoraFMS and its sub-folders, allowing standard users to create new files. Moreover, the Apache service httpd.exe will try to execute cmd.exe from C:\PandoraFMS (the current directory) as NT AUTHORITY\SYSTEM upon web requests to the portal. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM.	2019-06-29	not yet calculated	CVE-2019-13035 MISC
panduit -- intravue	An insecure login process was discovered in Panduit IntraVUE before 3.2.0.	2019-06-29	not yet calculated	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				13044 MISC
pulse_secure -- pulse_connect_secure	An input validation issue has been found with login_meeting.cgi in Pulse Secure Pulse Connect Secure 8.3RX before 8.3R2.	2019-06-28	not yet calculated	CVE-2018-20813 CONFIRM
pulse_secure -- pulse_connect_secure	An XSS issue has been found in welcome.cgi in Pulse Secure Pulse Connect Secure (PCS) 8.1.x before 8.1R12, 8.2.x before 8.2R9, and 8.3.x before 8.3R3 due to one of the URL parameters not being sanitized properly.	2019-06-28	not yet calculated	CVE-2018-20807 CONFIRM
pulse_secure -- pulse_connect_secure	An XSS issue was found with Psaldownload.cgi in Pulse Secure Pulse Connect Secure (PCS) 8.3R2 before 8.3R2 and Pulse Policy Secure (PPS) 5.4RX before 5.4R2. This is not applicable to PCS 8.1RX or PPS 5.2RX.	2019-06-28	not yet calculated	CVE-2018-20814 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pulse_secure -- pulse_connect_secure	An XSS issue has been found with rd.cgi in Pulse Secure Pulse Connect Secure 8.3RX before 8.3R3 due to improper header sanitization. This is not applicable to 8.1RX.	2019-06-28	not yet calculated	CVE-2018-20808 CONFIRM
pulse_secure -- pulse_connect_secure	A hidden RPC service issue was found with Pulse Secure Pulse Connect Secure 8.3RX before 8.3R2 and 8.1RX before 8.1R12.	2019-06-28	not yet calculated	CVE-2018-20811 CONFIRM
pulse_secure -- pulse_connect_secure_and_pulse_policy_secure	A crafted message can cause the web server to crash with Pulse Secure Pulse Connect Secure (PCS) 8.3RX before 8.3R5 and Pulse Policy Secure 5.4RX before 5.4R5. This is not applicable to PCS 8.1RX.	2019-06-28	not yet calculated	CVE-2018-20809 CONFIRM
pulse_secure -- pulse_connect_secure_and_pulse_policy_secure	Session data between cluster nodes during cluster synchronization is not properly encrypted in Pulse Secure Pulse Connect Secure (PCS) 8.3RX before 8.3R2 and Pulse Policy Secure (PPS) 5.4RX before 5.4R2. This is not applicable to PCS 8.1RX, PPS 5.2RX, or stand-alone devices.	2019-06-28	not yet calculated	CVE-2018-20810 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pulse_secure -- pulse_secure_desktop	An information exposure issue where IPv6 DNS traffic would be sent outside of the VPN tunnel (when Traffic Enforcement was enabled) exists in Pulse Secure Pulse Secure Desktop 9.0R1 and below. This is applicable only to dual-stack (IPv4/IPv6) endpoints.	2019-06-28	not yet calculated	CVE-2018-20812 CONFIRM
quadbase_systems -- espressreport_es	CSRF within the admin panel in Quadbase EspressReport ES (ERES) v7.0 update 7 allows remote attackers to escalate privileges, or create new admin accounts by crafting a malicious web page that issues specific requests, using a target admin's session to process their requests.	2019-06-24	not yet calculated	CVE-2019-9958 MISC
rockoa -- rockoa	RockOA 1.8.7 allows remote attackers to obtain sensitive information because the webmain/webmainAction.php publictreestore method constructs a SQL WHERE clause unsafely by using the pidfields and idfields parameters, aka background SQL injection.	2019-06-28	not yet calculated	CVE-2019-9846 MISC
seeddms -- seeddms	A stored XSS vulnerability was found in SeedDMS 5.1.11 due to poorly escaping the search result in the autocomplete search form	2019-06-28	not yet calculated	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	placed in the header of out/out.Viewfolder.php.			12932 MISC
sks_keyserver_project -- sks_keyserver	Interaction between the sks-keyserver code through 1.2.0 of the SKS keyserver network, and GnuPG through 2.2.16, makes it risky to have a GnuPG keyserver configuration line referring to a host on the SKS keyserver network. Retrieving data from this network may cause a persistent denial of service, because of a Certificate Spamming Attack.	2019-06-29	not yet calculated	CVE-2019-13050 MISC
toaruos -- toaruos	linker/linker.c in ToaruOS through 1.10.9 has insecure LD_LIBRARY_PATH handling in setuid applications.	2019-06-29	not yet calculated	CVE-2019-13046 MISC
toaruos -- toaruos	kernel/sys/syscall.c in ToaruOS through 1.10.9 has incorrect access control in sys_sysfunc case 9 for TOARU_SYS_FUNC_SETHEAP, allowing arbitrary kernel pages to be mapped into user land, leading to root access.	2019-06-29	not yet calculated	CVE-2019-13047 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
toaruos -- toaruos	kernel/sys/syscall.c in ToaruOS through 1.10.9 allows a denial of service upon a critical error in certain sys_sbrk allocation patterns (involving PAGE_SIZE, and a value less than PAGE_SIZE).	2019-06-29	not yet calculated	CVE-2019-13048 MISC
toaruos -- toaruos	An integer wrap in kernel/sys/syscall.c in ToaruOS 1.10.10 allows users to map arbitrary kernel pages into userland process space via TOARU_SYS_FUNC_MMAP, leading to escalation of privileges.	2019-06-29	not yet calculated	CVE-2019-13049 MISC
uninett -- mod_auth_mellon	mod_auth_mellon through 0.14.2 has an Open Redirect via the login?ReturnTo= substring, as demonstrated by omitting the // after http: in the target URL.	2019-06-29	not yet calculated	CVE-2019-13038 MISC
virt-cdi-cloner -- virt-cdi-cloner	A flaw was found in the containerized-data-importer in virt-cdi-cloner, version 1.4, where the host-assisted cloning feature does not determine whether the requesting user has permission to access the Persistent Volume Claim (PVC) in the source namespace. This could allow users to clone any PVC in the	2019-06-28	not yet calculated	CVE-2019-10175 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cluster into their own namespace, effectively allowing access to other user's data.			
wordpress -- wordpress	In the miniOrange SAML SP Single Sign On plugin before 4.8.73 for WordPress, the SAML Login Endpoint is vulnerable to XSS via a specially crafted SAMLResponse XML post.	2019-06-24	not yet calculated	CVE-2019-12346 MISC MISC
zoneminder -- zoneminder	Stored XSS in the Filters page (Name field) in ZoneMinder 1.32.3 allows a malicious user to embed and execute JavaScript code in the browser of any user who navigates to this page.	2019-06-29	not yet calculated	CVE-2019-13072 MISC