Vulnerability Summary for the Week of July 24, 2017

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

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
appsec-labs -- appsec_labs	AppUse 4.0 allows shell command injection via a proxy field.	2017-07-25	7.2	CVE-2017-11566 MISC(link is external)
buffalo -- wapm-1166d_firmware	WAPM-1166D firmware Ver.1.2.7 and earlier, WAPM-APG600H firmware Ver.1.16.1 and earlier allows remote attackers to bypass authentication and access the configuration interface via unspecified vectors.	2017-07-21	10.0	CVE-2017-2126 CONFIRM(link is external) JVN(link is external)
finecms -- finecms	dayrui FineCms 5.0.9 has SQL Injection via the num parameter in an action=related or action=tags request to libraries/Template.php.	2017-07-23	7.5	CVE-2017-11582 MISC(link is external)
finecms -- finecms	dayrui FineCms 5.0.9 has SQL Injection via the catid parameter in an action=related request to libraries/Template.php.	2017-07-23	7.5	CVE-2017-11583 MISC(link is external)
finecms -- finecms	dayrui FineCms 5.0.9 has SQL Injection via the field parameter in an action=module, action=member, action=form, or action=related request to libraries/Template.php.	2017-07-23	7.5	CVE-2017-11584 MISC(link is external)
finecms -- finecms	dayrui FineCms 5.0.9 has remote PHP code execution via the param parameter in an action=cache request to libraries/Template.php, aka Eval Injection.	2017-07-23	7.5	CVE-2017-11585 MISC(link is external)
fortinet -- fortiwlm	A hard-coded account named 'upgrade' in Fortinet FortiWLM 8.3.0 and lower versions	2017-07-22	7.5	CVE-2017-7336 BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows a remote attacker to log-in and execute commands with 'upgrade' account privileges.			CONFIRM(link is external)
geutebrueck -- gcore	Stack-based buffer overflow in GCoreServer.exe in the server in Geutebrueck Gcore 1.3.8.42 and 1.4.2.37 allows remote attackers to execute arbitrary code via a long URI in a GET request.	2017-07-21	7.5	CVE-2017-11517 EXPLOIT-DB(link is external)
greenpacket -- dx-350_firmware	Green Packet DX-350 Firmware version v2.8.9.5-g1.4.8-atheeb has a default password of admin for the admin account.	2017-07-21	7.5	CVE-2017-9932 MISC(link is external)
greenpacket -- dx-350_firmware	In Green Packet DX-350 Firmware version v2.8.9.5-g1.4.8-atheeb, the "PING" (aka tag_ipPing) feature within the web interface allows performing command injection, via the "pip" parameter.	2017-07-21	7.5	CVE-2017-9980 MISC(link is external)
imagemagick -- imagemagick	Memory leak in AcquireVirtualMemory in ImageMagick before 7 allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors.	2017-07-25	7.8	CVE-2016-7539 CONFIRM MLIST(link is external) BID(link is external) CONFIRM CONFIRM(link is external) CONFIRM(link is external)
imagemagick -- imagemagick	The ReadOneJNGImage function in coders/png.c in ImageMagick through 6.9.9-0 and 7.x through 7.0.6-1 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a malformed JNG file.	2017-07-21	7.1	CVE-2017-11505 CONFIRM CONFIRM(link is external)
imagemagick -- imagemagick	The ReadTXTImage function in coders/txt.c in ImageMagick through 6.9.9-0 and 7.x through 7.0.6-1 allows remote attackers to cause a denial of service (infinite loop) via a crafted file, because the end-of-file condition is not considered.	2017-07-22	7.1	CVE-2017-11523 CONFIRM CONFIRM(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM(link is external)
imagemagick -- imagemagick	The ReadCINImage function in coders/cin.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (memory consumption) via a crafted file.	2017-07-22	7.1	CVE-2017-11525 BID(link is external) CONFIRM CONFIRM(link is external)
imagemagick -- imagemagick	The ReadOneMNGImage function in coders/png.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a crafted file.	2017-07-22	7.1	CVE-2017-11526 BID(link is external) CONFIRM CONFIRM(link is external)
imagemagick -- imagemagick	The ReadDPXImage function in coders/dpx.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (memory consumption) via a crafted file.	2017-07-22	7.1	CVE-2017-11527 CONFIRM CONFIRM(link is external)
imagemagick -- imagemagick	The ReadEPTImage function in coders/ept.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (memory consumption) via a crafted file.	2017-07-22	7.1	CVE-2017-11530 CONFIRM CONFIRM(link is external)
inmarsat -- amosconnect_8	Hard-coded credentials in AmosConnect 8 allow remote attackers to gain full administrative privileges, including the ability to execute commands on the Microsoft Windows host platform with SYSTEM privileges by abusing AmosConnect Task Manager.	2017-07-22	10.0	CVE-2017-3222 BID(link is external) CERT-VN
libinfinity_project -- libinfinity	libinfinity before 0.6.6-1 does not validate expired SSL certificates, which allows remote attackers to have unspecified impact via unknown vectors.	2017-07-21	7.5	CVE-2015-3886 MLIST CONFIRM CONFIRM(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM(link is external)
rootkit_hunter_project -- rkhunter	rkhunter versions before 1.4.4 are vulnerable to file download over insecure channel when doing mirror update resulting into potential remote code execution.	2017-07-21	7.5	CVE-2017-7480 MLIST
sony -- wg-c10_firmware	WG-C10 v3.0.79 and earlier allows an attacker to execute arbitrary OS commands via unspecified vectors.	2017-07-21	9.0	CVE-2017-2275 MISC(link is external) JVN(link is external)
sony -- wg-c10_firmware	Buffer overflow in WG-C10 v3.0.79 and earlier allows an attacker to execute arbitrary commands via unspecified vectors.	2017-07-21	9.0	CVE-2017-2276 MISC(link is external) JVN(link is external)
tcpdump -- tcpdump	tcpdump 4.9.0 has a heap-based buffer over-read in the lldp_print function in print-lldp.c, related to util-print.c.	2017-07-22	7.5	CVE-2017-11541 BID(link is external) MISC(link is external)
tcpdump -- tcpdump	tcpdump 4.9.0 has a heap-based buffer over-read in the pimv1_print function in print-pim.c.	2017-07-22	7.5	CVE-2017-11542 BID(link is external) MISC(link is external)
tcpdump -- tcpdump	tcpdump 4.9.0 has a buffer overflow in the sliplink_print function in print-sl.c.	2017-07-22	7.5	CVE-2017-11543 BID(link is external) MISC(link is external)
tilde_cms_project -- tilde_cms	An issue was discovered in Tilde CMS 1.0.1. Due to missing escaping of the backtick character, a SELECT query in class.SystemAction.php is vulnerable to SQL Injection. The vulnerability can be triggered via a POST request to	2017-07-24	7.5	CVE-2017-11324 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/actionphp/action.input.php with the id parameter.			

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ansible -- ansible	Ansible versions 2.2.3 and earlier are vulnerable to an information disclosure flaw due to the interaction of call back plugins and the no_log directive where the information may not be sanitized properly.	2017-07-21	5.0	CVE-2017-7473 MISC(link is external)
atmail -- atmail	Cross-site scripting (XSS) vulnerability in atmail prior to version 7.8.0.2 allows remote attackers to inject arbitrary web script or HTML within the body of an email via an IMG element with both single quotes and double quotes.	2017-07-25	4.3	CVE-2017-11617 MISC(link is external) MISC(link is external)
atutor -- atutor	Directory Traversal exists in ATutor before 2.2.2 via the icon parameter to /mods/_core/courses/users/create_course.php. The attacker can read an arbitrary file by visiting get_course_icon.php?id= after the traversal attack.	2017-07-22	5.0	CVE-2016-10400 MISC(link is external) MISC(link is external)
buffalotech -- wmr-433w_firmware	Cross-site scripting vulnerability in WMR-433 firmware Ver.1.02 and earlier, WMR-433W firmware Ver.1.40 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-07-21	4.3	CVE-2017-2274 CONFIRM(link is external) JVN(link is external)
canonical -- ubuntu_linux	The simulate dbus method in aptdaemon before 1.1.1+bzr982-0ubuntu3.1 as packaged in Ubuntu 15.04, before 1.1.1+bzr980-0ubuntu1.1 as packaged in Ubuntu 14.10, before 1.1.1-1ubuntu5.2 as packaged in Ubuntu 14.04 LTS, before 0.43+bzr805-0ubuntu10 as	2017-07-21	4.9	CVE-2015-1323 BID(link is external) UBUNTU(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	packaged in Ubuntu 12.04 LTS allows local users to obtain sensitive information, or access files with root permissions.			
cisco -- prime_collaboration_provisioning	A vulnerability in the web portal of the Cisco Prime Collaboration Provisioning (PCP) Tool could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web interface of an affected system. More Information: CSCvc90312. Known Affected Releases: 12.1.	2017-07-25	4.3	CVE-2017-6755 BID(link is external) SECTRACK(link is external) CONFIRM(link is external)
contao -- contao_cms	Contao before 3.5.28 and 4.x before 4.4.1 allows remote attackers to include and execute arbitrary local PHP files via a crafted parameter in a URL, aka Directory Traversal.	2017-07-21	6.5	CVE-2017-10993 CONFIRM
cygwin -- cygwin	Cygwin versions 1.7.2 up to and including 1.8.0 are vulnerable to buffer overflow vulnerability in wcsxfrm/wcsxfrm_l functions resulting into denial-of-service by crashing the process or potential hijack of the process running with administrative privileges triggered by specially crafted input string.	2017-07-21	5.0	CVE-2017-7523 MISC(link is external)
ektron -- ektron_content_management_system	Cross-site scripting (XSS) vulnerability in Ektron Content Management System before 9.1.0.184SP3(9.1.0.184.3.127) allows remote attackers to inject arbitrary web script or HTML via the rptStatus parameter in a Report action to WorkArea/SelectUserGroup.aspx.	2017-07-25	4.3	CVE-2016-6133 BUGTRAQ(link is external)
eshop_project -- eshop	The eshop_checkout function in checkout.php in the Wordpress Eshop plugin 6.3.11 and earlier does not validate variables in the "eshopcart" HTTP cookie, which allows remote attackers to perform cross-site scripting	2017-07-21	4.3	CVE-2015-3421 BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(XSS) attacks, or a path disclosure attack via crafted variables named after target PHP variables.			MISC(link is external)
exiv2 -- exiv2	There is an illegal address access in the extend_alias_table function in localealias.c of Exiv2 0.26. A crafted input will lead to remote denial of service.	2017-07-22	5.0	CVE-2017-11553 MISC(link is external)
exiv2 -- exiv2	There is a Floating point exception in the Exiv2::ValueType function in Exiv2 0.26 that will lead to a remote denial of service attack via crafted input.	2017-07-23	5.0	CVE-2017-11591 MISC(link is external)
exiv2 -- exiv2	There is a Mismatched Memory Management Routines vulnerability in the Exiv2::FileIo::seek function of Exiv2 0.26 that will lead to a remote denial of service attack (heap memory corruption) via crafted input.	2017-07-23	5.0	CVE-2017-11592 MISC(link is external)
fedoraproject -- fedora	The log_config_command function in ntp_parser.y in ntpd in NTP before 4.2.7p42 allows remote attackers to cause a denial of service (ntpd crash) via crafted logconfig commands.	2017-07-21	5.0	CVE-2015-5194 CONFIRM FEDORA FEDORA SUSE SUSE SUSE REDHAT(link is external) REDHAT(link is external) DEBIAN MLIST(link is external) BID(link is external) UBUNTU(link is external) CONFIRM(link is external) CONFIRM(lin

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				k is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)
fedoraproject -- fedora	ntp_openssl.m4 in ntpd in NTP before 4.2.7p112 allows remote attackers to cause a denial of service (segmentation fault) via a crafted statistics or filegen configuration command that is not enabled during compilation.	2017-07-21	5.0	CVE-2015-5195 FEDORA FEDORA FEDORA REDHAT(link is external) REDHAT(link is external) DEBIAN MLIST(link is external) BID(link is external) UBUNTU(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fedoraproject -- fedora	The ULOGTOD function in ntp.d in SNTP before 4.2.7p366 does not properly perform type conversions from a precision value to a double, which allows remote attackers to cause a denial of service (infinite loop) via a crafted NTP packet.	2017-07-21	5.0	CVE-2015-5219 CONFIRM(link is external) CONFIRM FEDORA FEDORA FEDORA SUSE SUSE REDHAT(link is external) REDHAT(link is external) DEBIAN MLIST(link is external) BID(link is external) UBUNTU(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)
fedoraproject -- fedora	Use-after-free vulnerability in the mif_process_cmpt function in libjasper/mif/mif_cod.c in the JasPer JPEG-2000 library before 1.900.2 allows remote attackers to cause a denial	2017-07-25	4.3	CVE-2015-5221 SUSE SUSE SUSE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of service (crash) via a crafted JPEG 2000 image file.			MLIST(link is external) REDHAT(link is external) CONFIRM(link is external) CONFIRM(link is external) FEDORA FEDORA FEDORA
finecms -- finecms	dayrui FineCms 5.0.9 has Cross Site Scripting (XSS) in admin/Login.php via a payload in the username field that does not begin with a '<' character.	2017-07-23	4.3	CVE-2017-11581 MISC(link is external)
finecms -- finecms	dayrui FineCms 5.0.9 has URL Redirector Abuse via the url parameter in a sync action, related to controllers/Weixin.php.	2017-07-23	5.8	CVE-2017-11586 MISC(link is external)
fontforge -- fontforge	FontForge 20161012 is vulnerable to a heap-based buffer over-read in readttfcopyrights (parsettf.c) resulting in DoS or code execution via a crafted otf file.	2017-07-23	6.8	CVE-2017-11569 MISC(link is external)
fontforge_project -- fontforge	FontForge 20161012 is vulnerable to a heap-based buffer over-read in PSCharStringToSplines (psread.c) resulting in DoS or code execution via a crafted otf file.	2017-07-23	6.8	CVE-2017-11568 MISC(link is external)
fontforge_project -- fontforge	FontForge 20161012 is vulnerable to a buffer over-read in umodenc (parsettf.c) resulting in DoS or code execution via a crafted otf file.	2017-07-23	6.8	CVE-2017-11570 MISC(link is external)
fontforge_project -- fontforge	FontForge 20161012 is vulnerable to a stack-based buffer overflow in addnibble (parsettf.c) resulting in DoS or code execution via a crafted otf file.	2017-07-23	6.8	CVE-2017-11571 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fontforge_project -- fontforge	FontForge 20161012 is vulnerable to a heap-based buffer over-read in readcfftopdicts (parsettf.c) resulting in DoS or code execution via a crafted otf file.	2017-07-23	6.8	CVE-2017-11572 MISC(link is external)
fontforge_project -- fontforge	FontForge 20161012 is vulnerable to a buffer over-read in ValidatePostScriptFontName (parsettf.c) resulting in DoS or code execution via a crafted otf file.	2017-07-23	6.8	CVE-2017-11573 MISC(link is external)
fontforge_project -- fontforge	FontForge 20161012 is vulnerable to a heap-based buffer overflow in readcffset (parsettf.c) resulting in DoS or code execution via a crafted otf file.	2017-07-23	6.8	CVE-2017-11574 MISC(link is external)
fontforge_project -- fontforge	FontForge 20161012 is vulnerable to a buffer over-read in strnmatch (char.c) resulting in DoS or code execution via a crafted otf file, related to a call from the readttfcopyrights function in parsettf.c.	2017-07-23	6.8	CVE-2017-11575 MISC(link is external)
fontforge_project -- fontforge	FontForge 20161012 does not ensure a positive size in a weight vector memcpy call in readcfftopdict (parsettf.c) resulting in DoS via a crafted otf file.	2017-07-23	4.3	CVE-2017-11576 MISC(link is external)
fontforge_project -- fontforge	FontForge 20161012 is vulnerable to a buffer over-read in getsid (parsettf.c) resulting in DoS or code execution via a crafted otf file.	2017-07-23	6.8	CVE-2017-11577 MISC(link is external)
gnome -- libgxps	There is a NULL pointer dereference in the caseless_hash function in gxps-archive.c in libgxps 0.2.5. A crafted input will lead to a remote denial of service attack.	2017-07-23	4.3	CVE-2017-11590 MISC(link is external)
greenpacket -- dx-350_firmware	Cross-Site Request Forgery (CSRF) exists in Green Packet DX-350 Firmware version v2.8.9.5-g1.4.8-atheeb, as demonstrated by a request to ajax.cgi that enables UPnP.	2017-07-21	6.8	CVE-2017-9930 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
greenpacket -- dx-350_firmware	Cross-Site Scripting (XSS) exists in Green Packet DX-350 Firmware version v2.8.9.5-g1.4.8-atheeb, as demonstrated by the action parameter to ajax.cgi.	2017-07-21	4.3	CVE-2017-9931 MISC(link is external)
ibm -- rhapsody_design_manager	IBM Rhapsody DM 5.0 and 6.0 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.	2017-07-24	4.9	CVE-2017-1287 CONFIRM(link is external) MISC(link is external)
ibm -- security_guardium	IBM Security Guardium 10.0 and 10.1 processes patches, image backups and other updates without sufficiently verifying the origin and integrity of the code. IBM X-Force ID: 124742.	2017-07-21	5.0	CVE-2017-1267 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- tririga_application_platform	Builder tools running in the IBM TRIRIGA Application Platform 3.3, 3.4, and 3.5 contains a vulnerability that could allow an authenticated user to execute Builder tool actions they do not have access to. IBM X-Force ID: 126864.	2017-07-21	6.5	CVE-2017-1371 CONFIRM(link is external) MISC(link is external)
ibm -- tririga_application_platform	Reports executed in the IBM TRIRIGA Application Platform 3.3, 3.4, and 3.5 contains a vulnerability that could allow an authenticated user to execute a report they do not have access to. IBM X-Force ID: 126866.	2017-07-21	6.5	CVE-2017-1373 CONFIRM(link is external) BID(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- tririga_application_platform	Sensitive data can be exposed in the IBM TRIRIGA Application Platform 3.3, 3.4, and 3.5 that can lead to an attacker gaining unauthorized access to the system. IBM X-Force ID: 126867.	2017-07-21	4.0	CVE-2017-1374 CONFIRM(link is external) MISC(link is external)
imagemagick -- imagemagick	The WriteOnePNGImage function in coders/png.c in ImageMagick through 6.9.9-0 and 7.x through 7.0.6-1 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.	2017-07-22	4.3	CVE-2017-11522 CONFIRM CONFIRM(link is external) CONFIRM(link is external)
imagemagick -- imagemagick	The WriteBlob function in MagickCore/blob.c in ImageMagick before 6.9.8-10 and 7.x before 7.6.0-0 allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted file.	2017-07-22	4.3	CVE-2017-11524 BID(link is external) CONFIRM CONFIRM(link is external)
imagemagick -- imagemagick	The ReadDIBImage function in coders/dib.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (memory leak) via a crafted file.	2017-07-22	4.3	CVE-2017-11528 CONFIRM CONFIRM(link is external)
imagemagick -- imagemagick	The ReadMATImage function in coders/mat.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (memory leak) via a crafted file.	2017-07-22	4.3	CVE-2017-11529 CONFIRM CONFIRM(link is external)
imagemagick -- imagemagick	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the WriteMPCImage() function in coders/mpc.c.	2017-07-22	4.3	CVE-2017-11532 CONFIRM(link is external)
imagemagick -- imagemagick	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the	2017-07-22	4.3	CVE-2017-11533 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WriteUILImage() function in coders/uil.c.			
imagemagick -- imagemagick	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the lite_font_map() function in coders/wmf.c.	2017-07-22	4.3	CVE-2017-11534 CONFIRM(link is external)
imagemagick -- imagemagick	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the WritePSImage() function in coders/ps.c.	2017-07-22	4.3	CVE-2017-11535 CONFIRM(link is external)
imagemagick -- imagemagick	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the WriteJP2Image() function in coders/jp2.c.	2017-07-22	4.3	CVE-2017-11536 CONFIRM(link is external)
imagemagick -- imagemagick	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Floating Point Exception (FPE) in the WritePALMImage() function in coders/palm.c, related to an incorrect bits-per-pixel calculation.	2017-07-22	4.3	CVE-2017-11537 CONFIRM(link is external)
imagemagick -- imagemagick	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the WriteOnePNGImage() function in coders/png.c.	2017-07-22	4.3	CVE-2017-11538 CONFIRM(link is external)
imagemagick -- imagemagick	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the ReadOnePNGImage() function in coders/png.c.	2017-07-22	4.3	CVE-2017-11539 BID(link is external) CONFIRM(link is external)
imagemagick -- imagemagick	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the GetPixelIndex() function, called from the WritePICONImage function in coders/xpm.c.	2017-07-22	4.3	CVE-2017-11540 BID(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
inmarsat -- amosconnect_8	Blind SQL injection in the AmosConnect 8 login form allows remote attackers to access user credentials, including user names and passwords.	2017-07-22	5.0	CVE-2017-3221 BID(link is external) CERT-VN
libexpat_project -- libexpat	XML External Entity vulnerability in libexpat 2.2.0 and earlier (Expat XML Parser Library) allows attackers to put the parser in an infinite loop using a malformed external entity definition from an external DTD.	2017-07-25	5.0	CVE-2017-9233 MLIST(link is external) BID(link is external) CONFIRM(link is external) CONFIRM(link is external)
libsass -- libsass	There is a stack consumption vulnerability in the lex function in parser.hpp (as used in sassc) in LibSass 3.4.5. A crafted input will lead to a remote denial of service.	2017-07-22	5.0	CVE-2017-11554 MISC(link is external) MISC(link is external)
libsass -- libsass	There is an illegal address access in the Eval::operator function in eval.cpp in LibSass 3.4.5. A crafted input will lead to a remote denial of service.	2017-07-22	5.0	CVE-2017-11555 MISC(link is external)
libsass -- libsass	There is a stack consumption vulnerability in the Parser::advanceToNextToken function in parser.cpp in LibSass 3.4.5. A crafted input may lead to remote denial of service.	2017-07-22	5.0	CVE-2017-11556 MISC(link is external)
libsass -- libsass	There is a heap based buffer over-read in LibSass 3.4.5, related to address 0xb4803ea1. A crafted input will lead to a remote denial of service attack.	2017-07-24	4.3	CVE-2017-11605 BID(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
libsass -- libsass	There is a heap-based buffer over-read in the Sass::Prelexer::re_linebreak function in lexer.cpp in LibSass 3.4.5. A crafted input will lead to a remote denial of service attack.	2017-07-24	4.3	CVE-2017-11608 MISC(link is external)
linux -- linux_kernel	The ip6_find_1stfragopt function in net/ipv6/output_core.c in the Linux kernel through 4.12.3 allows local users to cause a denial of service (integer overflow and infinite loop) by leveraging the ability to open a raw socket.	2017-07-21	4.9	CVE-2017-7542 CONFIRM BID(link is external) CONFIRM(link is external)
microsec -- e-szigno	Microsec e-Szigno before 3.2.7.12 allows remote attackers to perform XML signature wrapping attacks via an e-akta signed document with a ds:Object node with a crafted payload prepended to a valid ds:Object.	2017-07-21	6.8	CVE-2015-3931 MISC(link is external) MISC BID(link is external) MISC(link is external) MISC(link is external) MISC(link is external)
netlock -- mokka	Netlock Mokka before 2.7.8.1204 allows remote attackers to perform XML signature wrapping attacks via an e-akta signed document with a ds:Object node with a crafted payload prepended to a valid ds:Object.	2017-07-21	6.8	CVE-2015-3932 MISC(link is external) MISC BID(link is external) MISC(link is external) MISC(link is external)
phpmybackuppro -- phpmybackuppro	phpMyBackupPro before 2.5 does not validate integer input, which allows remote authenticated users to execute arbitrary PHP code by injecting scripts	2017-07-21	6.5	CVE-2015-3638 MLIST(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	via the path, filename, and period parameters to scheduled.php, and making requests to injected scripts, or by injecting PHP into a PHP configuration variable via a PHP variable variable.			MLIST(link is external) SECTRACK(link is external)
phpmybackuppro -- phpmybackuppro	phpMyBackupPro 2.5 and earlier does not properly sanitize input strings, which allows remote authenticated users to execute arbitrary PHP code by storing a crafted string in a user configuration file.	2017-07-21	6.5	CVE-2015-3639 MLIST(link is external) MLIST(link is external) SECTRACK(link is external)
phpmybackuppro -- phpmybackuppro	phpMyBackupPro 2.5 and earlier does not properly escape the "." character in request parameters, which allows remote authenticated users with knowledge of a web-accessible and web-writeable directory on the target system to inject and execute arbitrary PHP scripts by injecting scripts via the path, filename, and dirs parameters to scheduled.php, and making requests to injected scripts.	2017-07-21	6.0	CVE-2015-3640 MLIST(link is external) SECTRACK(link is external)
sap -- netweaver_portal	Cross-site scripting (XSS) vulnerability in the DataArchivingService servlet in SAP NetWeaver Portal 7.4 allows remote attackers to inject arbitrary web script or HTML via the responsecode parameter to shp/shp_result.jsp, aka SAP Security Note 2308535.	2017-07-25	4.3	CVE-2017-11460 BID(link is external) MISC(link is external)
subsonic -- subsonic	Multiple cross-site request forgery (CSRF) vulnerabilities in the Podcast feature in Subsonic 6.1.1 allow remote attackers to hijack the authentication of users for requests that (1) subscribe to a podcast via the add parameter to podcastReceiverAdmin.view or (2) update Internet Radio Settings via the urlRedirectCustomUrl parameter to	2017-07-25	6.8	CVE-2017-9413 MISC(link is external) EXPLOIT-DB(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	networkSettings.view. NOTE: These vulnerabilities can be exploited to conduct server-side request forgery (SSRF) attacks.			
subsonic -- subsonic	Cross-site request forgery (CSRF) vulnerability in subsonic 6.1.1 allows remote attackers with knowledge of the target username to hijack the authentication of users for requests that change passwords via a crafted request to userSettings.view.	2017-07-21	5.1	CVE-2017-9415 EXPLOIT-DB(link is external)
tcpdump -- tcpdump	tcpdump 4.9.0 has a Segmentation Violation in the compressed_sl_print function in print-sl.c:229:3.	2017-07-22	5.0	CVE-2017-11544 BID(link is external) MISC(link is external)
tcpdump -- tcpdump	tcpdump 4.9.0 has a Segmentation Violation in the compressed_sl_print function in print-sl.c:253:34.	2017-07-22	5.0	CVE-2017-11545 BID(link is external) MISC(link is external)
tilde_cms_project -- tilde_cms	An issue was discovered in Tilde CMS 1.0.1. It is possible to bypass the implemented restrictions on arbitrary file upload via a filename.+php manipulation.	2017-07-24	5.0	CVE-2017-11326 MISC
tilde_cms_project -- tilde_cms	An issue was discovered in Tilde CMS 1.0.1. It is possible to retrieve sensitive data by using direct references. A low-privileged user can load PHP resources such as admin/content.php and admin/content.php?method=ftp_upload.	2017-07-24	4.0	CVE-2017-11327 MISC
tp-link -- archer_c9_(2.0)_firmware	passwd_recovery.lua on the TP-Link Archer C9(UN)_V2_160517 allows an attacker to reset the admin password by leveraging a predictable random number	2017-07-21	5.0	CVE-2017-11519 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	generator seed. This is fixed in C9(UN)_V2_170511.			MISC(link is external)
tukaani -- xz	scripts/xzgrep.in in xzgrep 5.2.x before 5.2.0, before 5.0.0 does not properly process file names containing semicolons, which allows remote attackers to execute arbitrary code by having a user run xzgrep on a crafted file name.	2017-07-25	4.6	CVE-2015-4035 MLIST MLIST(link is external) CONFIRM(link is external) CONFIRM
yiiframework -- yii	An XSS vulnerability exists in framework/views/errorHandler/exception.php in Yii Framework 2.0.12 affecting the exception screen when debug mode is enabled, because $exception->errorInfo is mishandled.	2017-07-21	4.3	CVE-2017-11516 CONFIRM(link is external) CONFIRM(link is external)

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- emptoris_strategic_supply_management	IBM Emptoris Supplier Lifecycle Management 10.1.0.x 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: 118356.	2017-07-24	3.5	CVE-2016-6118 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- rational_software_architect_design_manager	IBM Rational Software Architect Design Manager 5.0 and 6.0 is	2017-07-24	3.5	CVE-2017-1245 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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: 124580.			MISC(link is external)
ibm -- rhapsody_design_manager	IBM Rhapsody DM 5.0 and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 118912.	2017-07-24	3.5	CVE-2016-8975 CONFIRM(link is external) MISC(link is external)
ibm -- rhapsody_design_manager	IBM Rhapsody DM 5.0 and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2017-07-24	3.5	CVE-2017-1249 CONFIRM(link is external) MISC(link is external)
ibm -- tririga_application_platform	IBM TRIRIGA Application Platform 3.3, 3.4, and 3.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary	2017-07-21	3.5	CVE-2017-1372 CONFIRM(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 126865.			
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 127151.	2017-07-24	3.5	CVE-2017-1380 CONFIRM(link is external) BID(link is external) SECTRACK(link is external) MISC(link is external)
ibm -- websphere_application_server	IBM WebSphere Application Server Proxy Server or On-demand-router (ODR) 7.0, 8.0, 8.5, 9.0 and could allow a local attacker to obtain sensitive information, caused by stale data being cached and then served. IBM X-Force ID: 127152.	2017-07-21	2.1	CVE-2017-1381 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 might create files using the default permissions instead of the customized permissions when custom startup	2017-07-24	3.6	CVE-2017-1382 CONFIRM(link is external) BID(link is external) SECTRACK(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	scripts are used. A local attacker could exploit this to gain access to files with an unknown impact. IBM X-Force ID: 127153.			MISC(link is external)
selinux_project -- selinux	selinux-policy when sysctl fs.protected_hardlinks are set to 0 allows local users to cause a denial of service (SSH login prevention) by creating a hardlink to /etc/passwd from a directory named .config, and updating selinux-policy.	2017-07-21	2.1	CVE-2015-3170 CONFIRM(link is external)
sos_project -- sos	sosreport 3.2 uses weak permissions for generated sosreport archives, which allows local users with access to /var/tmp/ to obtain sensitive information by reading the contents of the archive.	2017-07-25	2.1	CVE-2015-3171 CONFIRM(link is external) CONFIRM(link is external)

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acunetix -- acunetix	Reporter.exe in Acunetix 8 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a malformed PRE file, related to a "User Mode Write AV starting at reporter!madTraceProcess."	2017-07-27	not yet calculated	CVE-2017-11673 MISC(link is external)
acunetix -- acunetix	Reporter.exe in Acunetix 8 allows remote attackers to cause a denial of service (application crash) via a	2017-07-27	not yet	CVE-2017-11674

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	malformed PRE file, related to a "Read Access Violation starting at reporter!madTraceProcess."		calculated	MISC(link is external)
airlink101 -- skyipcam1620w_wireless_n_mpeg4_3gpp_network_camera	snwrite.cgi in AirLink101 SkyIPCam1620W Wireless N MPEG4 3GPP network camera with firmware FW_AIC1620W_1.1.0-12_20120709_r1192.pck allows remote authenticated users to execute arbitrary OS commands via shell metacharacters in the mac parameter.	2017-07-24	not yet calculated	CVE-2015-2280 MISC(link is external) FULLDISC BUGTRAQ(link is external) BID(link is external) MISC(link is external) EXPLOIT-DB(link is external)
airlive -- multiple_products	cgi_test.cgi in AirLive BU-2015 with firmware 1.03.18, BU-3026 with firmware 1.43, and MD-3025 with firmware 1.81 allows remote attackers to execute arbitrary OS commands via shell metacharacters after an "&" (ampersand) in the write_mac write_pid, write_msn, write_tan, or write_hdv parameter.	2017-07-24	not yet calculated	CVE-2015-2279 MISC(link is external) FULLDISC BUGTRAQ(link is external) BID(link is external) MISC(link is external) EXPLOIT-DB(link is external)
apache -- activemq_artemis	XML external entity (XXE) vulnerability in the XPath selector component in Artemis ActiveMQ before commit 48d9951d879e0c8cbb59d4b64ab59d53ef88310d allows remote attackers to have unspecified impact via unknown vectors.	2017-07-25	not yet calculated	CVE-2015-3208 MLIST(link is external) BID(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				(link is external) CONFIRM (link is external)
apache -- http_server	---------- ---------- WARNING - CVE-2016-0736 was assigned by redhat, not apache! Description from apache : In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.	2017-07-27	not yet calculated	CVE-2016-0736 MISC
apache -- http_server	---------- ---------- WARNING - CVE-2016-2161 was assigned by redhat, not apache! Description from apache : In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.	2017-07-27	not yet calculated	CVE-2016-2161 MISC
apache -- http_server	---------- ---------- WARNING - a refinement exists for CVE-2016-8743 : theall/20170425-084430 (delay queue)! Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and	2017-07-27	not yet calculated	CVE-2016-8743 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	may result in request smuggling, response splitting and cache pollution.			
appserver -- appserver	Directory traversal vulnerability in the web request/response interface in Appserver before 1.0.3 allows remote attackers to read normally inaccessible files via a .. (dot dot) in a crafted URL.	2017-07-24	not yet calculated	CVE-2015-1847 CONFIRM (link is external)
artifex -- artifex_ghostscript	psi/ztoken.c in Artifex Ghostscript 9.21 mishandles references to the scanner state structure, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PostScript document, related to an out-of-bounds read in the igc_reloc_struct_ptr function in psi/igc.c.	2017-07-28	not yet calculated	CVE-2017-11714 CONFIRM (link is external) CONFIRM (link is external)
artifex -- artifex_ghostscript_ghostxps	The Ins_MIRP function in base/ttinterp.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.	2017-07-26	not yet calculated	CVE-2017-9611 CONFIRM (link is external) CONFIRM (link is external)
artifex -- artifex_ghostscript_ghostxps	The xps_select_font_encoding function in xps/xpsfont.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document, related to the xps_encode_font_char_imp function.	2017-07-26	not yet calculated	CVE-2017-9620 CONFIRM (link is external) CONFIRM (link is external)
artifex -- artifex_ghostscript_ghostxps	The xps_true_callback_glyph_name function in xps/xpsttf.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (Segmentation Violation and application crash) via a crafted file.	2017-07-26	not yet calculated	CVE-2017-9619 CONFIRM (link is external) CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
artifex -- artifex_ghostscript_ghostxps	The xps_load_sfnt_name function in xps/xpsfont.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted document.	2017-07-26	not yet calculated	CVE-2017-9618 CONFIRM (link is external) CONFIRM (link is external)
artifex -- artifex_ghostscript_ghostxps	The xps_decode_font_char_imp function in xps/xpsfont.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.	2017-07-26	not yet calculated	CVE-2017-9740 CONFIRM (link is external) CONFIRM (link is external)
artifex -- artifex_ghostscript_ghostxps	The gx_ttfReader__Read function in base/gxttfb.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.	2017-07-26	not yet calculated	CVE-2017-9727 CONFIRM (link is external) CONFIRM (link is external)
artifex -- artifex_ghostscript_ghostxps	The Ins_IP function in base/ttinterp.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via a crafted document.	2017-07-26	not yet calculated	CVE-2017-9612 CONFIRM (link is external) CONFIRM (link is external)
artifex -- artifex_ghostscript_ghostxps	The Ins_JMPR function in base/ttinterp.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.	2017-07-26	not yet calculated	CVE-2017-9739 CONFIRM (link is external) CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
artifex -- artifex_ghostscript_ghostxps	The xps_load_sfnt_name function in xps/xpsfont.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.	2017-07-26	not yet calculated	CVE-2017-9610 CONFIRM (link is external) CONFIRM (link is external)
artifex -- artifex_ghostscript_ghostxps	The Ins_MDRP function in base/ttinterp.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.	2017-07-26	not yet calculated	CVE-2017-9726 CONFIRM (link is external) CONFIRM (link is external)
artifex -- artifex_ghostscript	The gs_alloc_ref_array function in psi/ialloc.c in Artifex Ghostscript 9.22 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted PostScript document. This is related to a lack of an integer overflow check in base/gsalloc.c.	2017-07-26	not yet calculated	CVE-2017-9835 CONFIRM (link is external) CONFIRM (link is external)
audiocoder -- audiocoder	Buffer overflow in AudioCoder 0.8.46 allows remote attackers to execute arbitrary code via a crafted .m3u file.	2017-07-27	not yet calculated	CVE-2017-8870 EXPLOIT-DB(link is external)
avira -- avira_antivirus	Avira Antivirus engine versions before 8.3.36.60 allow remote code execution as NT AUTHORITY\SYSTEM via a section header with a very large relative virtual address in a PE file, causing an integer overflow and heap-based buffer underflow.	2017-07-27	not yet calculated	CVE-2016-10402 MISC
cacti -- cacti	Cross-site scripting (XSS) vulnerability in auth_profile.php in Cacti 1.1.13 allows remote attackers to inject arbitrary web	2017-07-27	not yet calculated	CVE-2017-11691 CONFIRM (link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	script or HTML via specially crafted HTTP Referer headers.			external) CONFIRM (link is external)
candlepin -- candlepin	Candlepin allows remote attackers to obtain sensitive information by obtaining Java exception statements as a result of excessive web traffic.	2017-07-25	not yet calculated	CVE-2015-5187 CONFIRM (link is external)
cisco -- asr_5000_series_aggregation_services_routers	A vulnerability in certain filtering mechanisms of access control lists (ACLs) for Cisco ASR 5000 Series Aggregation Services Routers through 21.x could allow an unauthenticated, remote attacker to bypass ACL rules that have been configured for an affected device. More Information: CSCvb99022 CSCvc16964 CSCvc37351 CSCvc54843 CSCvc63444 CSCvc77815 CSCvc88658 CSCve08955 CSCve14141 CSCve33870.	2017-07-25	not yet calculated	CVE-2017-6672 BID(link is external) SECTRAC K(link is external) CONFIRM (link is external)
cisco -- asr_5000_series_aggregation_services_routers	A vulnerability in the gateway GPRS support node (GGSN) of Cisco ASR 5000 Series Aggregation Services Routers 17.3.9.62033 through 21.1.2 could allow an unauthenticated, remote attacker to redirect HTTP traffic sent to an affected device. More Information: CSCvc67927.	2017-07-25	not yet calculated	CVE-2017-6612 BID(link is external) SECTRAC K(link is external) CONFIRM (link is external)
cisco -- cloud_web_security	Cross-site scripting (XSS) vulnerability in the Alert Service of Cisco Cloud Web Security base revision allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.	2017-07-25	not yet calculated	CVE-2015-0674 CISCO(link is external)
cisco -- residential_gateway	On Cisco DDR2200 ADSL2+ Residential Gateway DDR2200B-NA-AnnexA-FCC-V00.00.03.45.4E and DDR2201v1 ADSL2+ Residential Gateway DDR2201v1-NA-AnnexA-FCC-V00.00.03.28.3 devices, there is	2017-07-23	not yet calculated	CVE-2017-11588 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote command execution via shell metacharacters in the pingAddr parameter to the waitPingqry.cgi URI. The command output is visible at /PingMsg.cmd.			BID(link is external)
cisco -- residential_gateway	On Cisco DDR2200 ADSL2+ Residential Gateway DDR2200B-NA-AnnexA-FCC-V00.00.03.45.4E and DDR2201v1 ADSL2+ Residential Gateway DDR2201v1-NA-AnnexA-FCC-V00.00.03.28.3 devices, there is no access control for info.html, wancfg.cmd, rtroutecfg.cmd, arpview.cmd, cpuview.cmd, memoryview.cmd, statswan.cmd, statsatm.cmd, scsrvcntr.cmd, scacccntr.cmd, logview.cmd, voicesipview.cmd, usbview.cmd, wlmacflt.cmd, wlwds.cmd, wlstationlist.cmd, HPNAShow.cmd, HPNAView.cmd, qoscls.cmd, qosqueue.cmd, portmap.cmd, scmacflt.cmd, scinflt.cmd, scoutflt.cmd, certlocal.cmd, or certca.cmd.	2017-07-23	not yet calculated	CVE-2017-11589 MISC
cisco -- residential_gateway	On Cisco DDR2200 ADSL2+ Residential Gateway DDR2200B-NA-AnnexA-FCC-V00.00.03.45.4E and DDR2201v1 ADSL2+ Residential Gateway DDR2201v1-NA-AnnexA-FCC-V00.00.03.28.3 devices, there is directory traversal in the filename parameter to the /download.conf URI.	2017-07-23	not yet calculated	CVE-2017-11587 MISC
cisco -- web_security_appliance	A vulnerability in AsyncOS for the Cisco Web Security Appliance (WSA) could allow an unauthenticated, local attacker to log in to the device with the privileges of a limited user or an unauthenticated, remote attacker to authenticate to certain areas of the web GUI, aka a Static Credentials Vulnerability. Affected Products: virtual and hardware versions of Cisco Web Security Appliance (WSA). More Information: CSCve06124.	2017-07-25	not yet calculated	CVE-2017-6750 BID(link is external) SECTRACK(link is external) CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Known Affected Releases: 10.1.0-204. Known Fixed Releases: 10.5.1-270.			
cisco -- web_security_appliance	A vulnerability in the web proxy functionality of the Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to forward traffic from the web proxy interface of an affected device to the administrative management interface of an affected device, aka an Access Control Bypass Vulnerability. Affected Products: virtual and hardware versions of Cisco Web Security Appliance (WSA). More Information: CSCvd88863. Known Affected Releases: 10.1.0-204 9.0.0-485.	2017-07-25	not yet calculated	CVE-2017-6751 BID(link is external) SECTRACK(link is external) CONFIRM (link is external)
cisco -- web_security_appliance	A vulnerability in the web interface of the Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to perform command injection and elevate privileges to root. The attacker must authenticate with valid administrator credentials. Affected Products: Cisco AsyncOS Software 10.0 and later for WSA on both virtual and hardware appliances. More Information: CSCvd88862. Known Affected Releases: 10.1.0-204. Known Fixed Releases: 10.5.1-270 10.1.1-235.	2017-07-25	not yet calculated	CVE-2017-6746 BID(link is external) SECTRACK(link is external) CONFIRM (link is external)
cisco -- web_security_appliance	A vulnerability in the CLI parser of the Cisco Web Security Appliance (WSA) could allow an authenticated, local attacker to perform command injection and elevate privileges to root. The attacker must authenticate with valid operator-level or administrator-level credentials. Affected Products: virtual and hardware versions of Cisco Web Security Appliance (WSA). More Information: CSCvd88855. Known Affected Releases: 10.1.0-204. Known Fixed Releases: 10.5.1-270 10.1.1-234.	2017-07-25	not yet calculated	CVE-2017-6748 BID(link is external) SECTRACK(link is external) CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- web_security_appliance	A vulnerability in the web-based management interface of Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. Affected Products: virtual and hardware versions of Cisco Web Security Appliance (WSA). More Information: CSCvd88865. Known Affected Releases: 10.1.0-204.	2017-07-25	not yet calculated	CVE-2017-6749 BID(link is external) SECTRACK(link is external) CONFIRM (link is external)
cisco --webex	A vulnerability in Cisco WebEx browser extensions for Google Chrome and Mozilla Firefox could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server, Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center), and Cisco WebEx Meetings when they are running on Microsoft Windows. The vulnerability is due to a design defect in the extension. An attacker who can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser. The following versions of the Cisco WebEx browser extensions are affected: Versions prior to 1.0.12 of the Cisco WebEx extension on Google Chrome, Versions prior to 1.0.12 of the Cisco WebEx extension on Mozilla Firefox. Cisco Bug IDs: CSCvf15012 CSCvf15020 CSCvf15030 CSCvf15033 CSCvf15036 CSCvf15037.	2017-07-25	not yet calculated	CVE-2017-6753 BID(link is external) SECTRACK(link is external) SECTRACK(link is external) SECTRACK(link is external) CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cloud_foundry -- capi_release	An issue was discovered in the Cloud Controller API in Cloud Foundry Foundation CAPI-release version 1.33.0 (only). The original fix for CVE-2017-8033 included in CAPI-release 1.33.0 introduces a regression that allows a space developer to execute arbitrary code on the Cloud Controller VM by pushing a specially crafted application.	2017-07-24	not yet calculated	CVE-2017-8036 CONFIRM
cloud_foundry -- capi_release	An issue was discovered in the Cloud Controller API in Cloud Foundry Foundation CAPI-release versions prior to v1.35.0 and cf-release versions prior to v268. A filesystem traversal vulnerability exists in the Cloud Controller that allows a space developer to escalate privileges by pushing a specially crafted application that can write arbitrary files to the Cloud Controller VM.	2017-07-25	not yet calculated	CVE-2017-8033 CONFIRM
cloud_foundry -- capi_release	An issue was discovered in the Cloud Controller API in Cloud Foundry Foundation CAPI-release versions after v1.6.0 and prior to v1.35.0 and cf-release versions after v244 and prior to v268. A carefully crafted CAPI request from a Space Developer can allow them to gain access to files on the Cloud Controller VM for that installation.	2017-07-25	not yet calculated	CVE-2017-8035 CONFIRM
dayrui -- dayrui	dayrui FineCms through 5.0.10 has Cross Site Scripting (XSS) in controllers/api.php via the function parameter in a c=api&m=data2 request.	2017-07-26	not yet calculated	CVE-2017-11629 MISC(link is external)
debian -- tor	debian/tor.init in the Debian tor_0.2.9.11-1~deb9u1 package for Tor was designed to execute aa-exec from the standard system pathname if the apparmor package is installed, but implements this incorrectly (with a wrong assumption that the specific pathname would remain the same forever), which allows attackers to	2017-07-23	not yet calculated	CVE-2017-11565 BID(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bypass intended AppArmor restrictions by leveraging the silent loss of this protection mechanism. NOTE: this does not affect systems, such as default Debian stretch installations, on which Tor startup relies on a systemd unit file (instead of this tor.init script).			
efront -- efront	Unrestricted file upload vulnerability in eFront CMS before 3.6.15.5 allows remote authenticated users to execute arbitrary code by uploading a file from a local URL, then accessing it via a direct request to the file in www/content/lessons/"lesson number"/"directory name".	2017-07-25	not yet calculated	CVE-2015-4462 CONFIRM (link is external) MISC(link is external)
efront -- efront	Unrestricted file upload vulnerability in eFront CMS before 3.6.15.5 allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension prepended to a crafted parameter, then accessing it via a direct request to the file in www/content/lessons/"lesson number"/"directory name".	2017-07-25	not yet calculated	CVE-2015-4463 CONFIRM (link is external) MISC(link is external)
exiv2 -- exiv2	There is a reachable assertion in the Internal::TiffReader::visitDirectory function in tiffvisitor.cpp of Exiv2 0.26 that will lead to a remote denial of service attack via crafted input.	2017-07-27	not yet calculated	CVE-2017-11683 MISC(link is external)
ffmpeg -- ffmpeg	The dnxhd_decode_header function in libavcodec/dnxhddec.c in FFmpeg through 3.3.2 allows remote attackers to cause a denial of service (out-of-array access) or possibly have unspecified other impact via a crafted DNxHD file.	2017-07-28	not yet calculated	CVE-2017-11719 CONFIRM (link is external)
ffmpeg -- ffmpeg	The ff_amf_get_field_value function in libavformat/rtmppkt.c in FFmpeg 3.3.2 allows remote RTMP servers to cause a denial of service (Segmentation Violation and application crash) via a crafted stream.	2017-07-27	not yet calculated	CVE-2017-11665 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fiyo -- fiyo	dapur/app/app_user/controller/status.php in Fiyo CMS 2.0.7 has SQL injection via the id parameter.	2017-07-26	not yet calculated	CVE-2017-11631 MISC(link is external)
fiyo -- fiyo	dapur\apps\app_config\controller\backuper.php in Fiyo CMS 2.0.7 allows remote attackers to delete arbitrary files via directory traversal sequences in the file parameter in a type=database request, a different vulnerability than CVE-2017-8853.	2017-07-26	not yet calculated	CVE-2017-11630 MISC(link is external)
foreman -- foreman	rubygem-safemode, as used in Foreman, versions 1.3.2 and earlier are vulnerable to bypassing safe mode limitations via special Ruby syntax. This can lead to deletion of objects for which the user does not have delete permissions or possibly to privilege escalation.	2017-07-21	not yet calculated	CVE-2017-7540 MISC(link is external)
freebsd -- freebsd	The inet module in FreeBSD 10.2x before 10.2-PRERELEASE, 10.2-BETA2-p2, 10.2-RC1-p1, 10.1x before 10.1-RELEASE-p16, 9.x before 9.3-STABLE, 9.3-RELEASE-p21, and 8.x before 8.4-STABLE, 8.4-RELEASE-p35 on systems with VNET enabled and at least 16 VNET instances allows remote attackers to cause a denial of service (mbuf consumption) via multiple concurrent TCP connections.	2017-07-25	not yet calculated	CVE-2015-1417 BID(link is external) SECTRAC K(link is external) FREEBSD
glpi -- glpi	SQL injection exists in front/devicesoundcard.php in GLPI before 9.1.5 via the start parameter.	2017-07-28	not yet calculated	CVE-2017-11184 CONFIRM (link is external) CONFIRM (link is external)
glpi -- glpi	front/backup.php in GLPI before 9.1.5 allows remote authenticated	2017-07-28	not yet	CVE-2017-11183

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	administrators to delete arbitrary files via a crafted file parameter.		calculated	CONFIRM (link is external) CONFIRM (link is external)
gnu -- gnu_compiler_collection	Under certain circumstances, the ix86_expand_builtin function in i386.c in GNU Compiler Collection (GCC) version 4.6, 4.7, 4.8, 4.9, 5 before 5.5, and 6 before 6.4 will generate instruction sequences that clobber the status flag of the RDRAND and RDSEED intrinsics before it can be read, potentially causing failures of these instructions to go unreported. This could potentially lead to less randomness in random number generation.	2017-07-26	not yet calculated	CVE-2017-11671 CONFIRM (link is external) CONFIRM CONFIRM
google -- chrome	Cross-site scripting (XSS) vulnerability in the Markdown Preview Plus extension before 0.5.7 for Chrome allows remote attackers to inject arbitrary web script or HTML into some web applications via the upload and display of crafted text, markdown, or rst files that are designed to be viewed in the browser as plain text, but that will be converted to HTML without proper sanitization.	2017-07-23	not yet calculated	CVE-2017-11593 CONFIRM (link is external) CONFIRM (link is external)
google --android	The Boozt Fashion application before 2.3.4 for Android allows remote attackers to read login credentials by sniffing the network and leveraging the lack of SSL. NOTE: the vendor response, before the application was changed to enable SSL logins, was "At the moment that is an accepted risk. We only have https on the checkout part of the site."	2017-07-28	not yet calculated	CVE-2017-11706 MISC(link is external) MISC(link is external)
graphicsmagick -- graphicsmagick	GraphicsMagick 1.3.26 has a NULL pointer dereference in the WriteMAPImage() function in coders/map.c when processing a non-	2017-07-26	not yet calculated	CVE-2017-11642 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	colormapped image, a different vulnerability than CVE-2017-11638.			(link is external)
graphicsmagick -- graphicsmagick	The WriteOnePNGImage function in coders/png.c in GraphicsMagick 1.3.26 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted file, because the program's actual control flow was inconsistent with its indentation. This resulted in a logging statement executing outside of a loop, and consequently using an invalid array index corresponding to the loop's exit condition.	2017-07-28	not yet calculated	CVE-2017-11722 MISC(link is external)
graphicsmagick -- graphicsmagick	GraphicsMagick 1.3.26 has a heap overflow in the WriteRGBImage() function in coders/rgb.c when processing multiple frames that have non-identical widths.	2017-07-26	not yet calculated	CVE-2017-11636 CONFIRM (link is external)
graphicsmagick -- graphicsmagick	GraphicsMagick 1.3.26 has a heap overflow in the WriteCMYKImage() function in coders/cmyk.c when processing multiple frames that have non-identical widths.	2017-07-26	not yet calculated	CVE-2017-11643 CONFIRM (link is external)
graphicsmagick -- graphicsmagick	GraphicsMagick 1.3.26 has a Memory Leak in the PersistCache function in magick/pixel_cache.c during writing of Magick Persistent Cache (MPC) files.	2017-07-26	not yet calculated	CVE-2017-11641 CONFIRM (link is external)
graphicsmagick -- graphicsmagick	GraphicsMagick 1.3.26 has a segmentation violation in the WriteMAPImage() function in coders/map.c when processing a non-colormapped image, a different vulnerability than CVE-2017-11642.	2017-07-26	not yet calculated	CVE-2017-11638 CONFIRM (link is external)
graphicsmagick -- graphicsmagick	GraphicsMagick 1.3.26 has a NULL pointer dereference in the WritePCLImage() function in	2017-07-26	not yet	CVE-2017-11637

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	coders/pcl.c during writes of monochrome images.		calculated	CONFIRM (link is external)
hangul -- hangul	hwpapp.dll in Hangul Word Processor allows remote attackers to execute arbitrary code via a crafted heap spray, and by leveraging a "type confusion" via an HWPX file containing a crafted para text tag.	2017-07-25	not yet calculated	CVE-2015-6585 CONFIRM (link is external) BID(link is external) CONFIRM (link is external) CONFIRM (link is external)
hashtopus -- hashtopus	SQL injection vulnerability in Hashtopus 1.5g allows remote authenticated users to execute arbitrary SQL commands via the format parameter in admin.php.	2017-07-27	not yet calculated	CVE-2017-11678 MISC(link is external)
hashtopus -- hashtopus	Cross-site scripting (XSS) vulnerability in Hashtopus 1.5g allows remote attackers to inject arbitrary web script or HTML via the query string to admin.php.	2017-07-27	not yet calculated	CVE-2017-11677 MISC(link is external)
hashtopus -- hashtopus	Cross-Site Request Forgery (CSRF) exists in Hashtopus 1.5g via the password parameter to admin.php in an a=config action.	2017-07-27	not yet calculated	CVE-2017-11679 MISC(link is external)
hashtopussy -- hashtopussy	Incorrect Access Control vulnerability in Hashtopussy 0.4.0 allows remote authenticated users to execute actions that should only be available for administrative roles, as demonstrated by an action=createVoucher request to agents.php.	2017-07-27	not yet calculated	CVE-2017-11681 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hashtopussy -- hashtopussy	Cross-Site Request Forgery (CSRF) exists in Hashtopussy 0.4.0, allowing an admin password change via users.php.	2017-07-27	not yet calculated	CVE-2017-11680 MISC(link is external)
hashtopussy -- hashtopussy	Stored Cross-site scripting vulnerability in Hashtopussy 0.4.0 allows remote attackers to inject arbitrary web script or HTML via the (1) version, (2) url, or (3) rootdir parameter in hashcat.php.	2017-07-27	not yet calculated	CVE-2017-11682 MISC(link is external)
imagemagick -- imagemagick	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to an address access exception in the WritePTIFImage() function in coders/tiff.c.	2017-07-26	not yet calculated	CVE-2017-11640 CONFIRM (link is external)
imagemagick -- imagemagick	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the WriteCIPImage() function in coders/cip.c, related to the GetPixelLuma function in MagickCore/pixel-accessor.h.	2017-07-26	not yet calculated	CVE-2017-11639 CONFIRM (link is external)
imagemagick -- imagemagick	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the WriteHISTOGRAMImage() function in coders/histogram.c.	2017-07-22	not yet calculated	CVE-2017-11531 CONFIRM (link is external)
imagemagick -- imagemagick	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the ReadMATImage() function in coders/mat.c.	2017-07-26	not yet calculated	CVE-2017-11644 CONFIRM (link is external)
intel -- intel_processors	Incorrect check in Intel processors from 6th and 7th Generation Intel Core Processor Families, Intel Xeon E3-1500M v5 and v6 Product Families, and Intel Xeon E3-1200 v5 and v6 Product Families allows compromised system	2017-07-26	not yet calculated	CVE-2017-5691 CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	firmware to impact SGX security via incorrect early system state.			
intense_pc -- phoenix_securecore_uefi	Intense PC (aka MintBox 2) Phoenix SecureCore UEFI firmware does not perform capsule signature validation before upgrading the system firmware. The absence of signature validation allows an attacker with administrator privileges to flash a modified UEFI BIOS.	2017-07-25	not yet calculated	CVE-2017-9457 MISC MISC(link is external)
joomla -- joomla!	In Joomla! before 3.7.4, inadequate filtering of potentially malicious HTML tags leads to XSS vulnerabilities in various components.	2017-07-26	not yet calculated	CVE-2017-11612 CONFIRM
joomla -- joomla!	SQL injection vulnerability in Joomla! Component Contact Form Maker 1.0.1 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2017-07-25	not yet calculated	CVE-2015-2798 BID(link is external) EXPLOIT-DB(link is external)
koha -- koha	Multiple cross-site request forgery (CSRF) vulnerabilities in Koha Libraries 3.20.x before 3.20.1, 3.14.x before 3.14.16, 3.16.x before 3.16.12 allow remote attackers to (1) hijack the authentication of users with access to the OPAC interface and who have permissions to create public lists for requests that inject arbitrary web script or HTML via the addshelf parameter to opac-shelves.pl, (2) hijack the authentication of users with access to the OPAC interface and who have permissions to create public lists for requests that inject arbitrary web script or HTML via an unspecified list name parameter to opac-addbybiblionumber.pl, (3) hijack the authentication of library administrator users for requests that execute arbitrary web script or HTML via virtualshelves/shelves.pl when a shelf	2017-07-21	not yet calculated	CVE-2015-4639 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	name contains web script or HTML, or (4) hijack the authentication of users with access to the OPAC interface and who have permissions to create public lists for requests that execute arbitrary web script or HTML by adding a biblio to a list whose name contains web script or HTML.			
kopano -- kopano	Cross-site scripting (XSS) vulnerability in js/ViewerPanel.js in the file previewer plugin in Kopano WebApp versions 3.3.0 and earlier allows remote attackers to inject arbitrary web script or HTML via a specially crafted previewable file.	2017-07-26	not yet calculated	CVE-2017-11666 CONFIRM (link is external)
lame -- lame	The fill_buffer_resample function in libmp3lame/util.c in LAME 3.99.5 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted wav file.	2017-07-27	not yet calculated	CVE-2017-9411 MISC
lame -- lame	The unpack_read_samples function in frontend/get_audio.c in LAME 3.99.5 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted wav file.	2017-07-27	not yet calculated	CVE-2017-9412 MISC
lame -- lame	The fill_buffer_resample function in libmp3lame/util.c in LAME 3.99.5 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted wav file.	2017-07-27	not yet calculated	CVE-2017-9410 MISC
lame --lame	There is a division-by-zero vulnerability in LAME 3.99.5, caused by a malformed input file.	2017-07-28	not yet calculated	CVE-2017-11720 MISC(link is external)
libav -- libav	There is an illegal address access in the build_table function in libavcodec/bitstream.c of Libav 12.1 that will lead to remote denial of service via crafted input.	2017-07-27	not yet calculated	CVE-2017-11684 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
libdeploypkg -- libdeploypkg	VMware Tools prior to 10.0.9 contains multiple file system races in libDeployPkg, related to the use of hard-coded paths under /tmp. Successful exploitation of this issue may result in a local privilege escalation.	2017-07-28	not yet calculated	CVE-2015-5191 CONFIRM (link is external)
libjpeg-turbo -- libjpeg-turbo	The fill_input_buffer function in jdatasrc.c in libjpeg-turbo 1.5.1 allows remote attackers to cause a denial of service (invalid memory access and application crash) or possibly have unspecified other impact via a crafted jpg file.	2017-07-27	not yet calculated	CVE-2017-9614 MISC
libtiff -- libtiff	In LibTIFF 4.0.8, there is a denial of service vulnerability in the TIFFOpen function. A crafted input will lead to a denial of service attack. During the TIFFOpen process, td_imagelength is not checked. The value of td_imagelength can be directly controlled by an input file. In the ChopUpSingleUncompressedStrip function, the _TIFFCheckMalloc function is called based on td_imagelength. If we set the value of td_imagelength close to the amount of system memory, it will hang the system or trigger the OOM killer.	2017-07-26	not yet calculated	CVE-2017-11613 MISC(link is external)
linux -- linux_kernel	The brcmf_cfg80211_mgmt_tx function in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux kernel before 4.12.3 allows local users to cause a denial of service (buffer overflow and system crash) or possibly gain privileges via a crafted NL80211_CMD_FRAME Netlink packet.	2017-07-25	not yet calculated	CVE-2017-7541 CONFIRM CONFIRM (link is external) CONFIRM BID(link is external) SECTRAC K(link is external) CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	net/xfrm/xfrm_policy.c in the Linux kernel through 4.12.3, when CONFIG_XFRM_MIGRATE is enabled, does not ensure that the dir value of xfrm_userpolicy_id is XFRM_POLICY_MAX or less, which allows local users to cause a denial of service (out-of-bounds access) or possibly have unspecified other impact via an XFRM_MSG_MIGRATE xfrm Netlink message.	2017-07-24	not yet calculated	CVE-2017-11600 MISC
locationvalue -- restaurant_karaoke_shidax	The Restaurant Karaoke SHIDAX app 1.3.3 and earlier on Android does not verify SSL certificates, which allows remote attackers to obtain sensitive information via a man-in-the-middle attack.	2017-07-25	not yet calculated	CVE-2015-0904 JVN(link is external) JVNDB(link is external)
loomio -- loomio	Cross-site scripting (XSS) vulnerability in the Markdown parser in Loomio before 1.8.0 allows remote attackers to inject arbitrary web script or HTML via non-sanitized Markdown content in a new thread or a thread comment.	2017-07-23	not yet calculated	CVE-2017-11594 CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
medhost -- connex	MEDHOST Connex contains hard-coded credentials that are used for customer database access. An attacker with	2017-07-25	not yet	CVE-2017-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	knowledge of the hard-coded credentials and the ability to communicate directly with the database may be able to obtain or modify sensitive patient and financial information. Connex utilizes an IBM i DB2 user account for database access. The account name is HMSCXPDN. Its password is hard-coded in multiple places in the application. Customers do not have the option to change this password. The account has elevated DB2 roles, and can access all objects or database tables on the customer DB2 database. This account can access data through ODBC, FTP, and TELNET. Customers without Connex installed are still vulnerable because the MEDHOST setup program creates this account.		calculated	11614 MISC
medhost -- medhost	MEDHOST Document Management System contains hard-coded credentials that are used for Apache Solr access. An attacker with knowledge of the hard-coded credentials and the ability to communicate directly with Apache Solr may be able to obtain or modify sensitive patient and financial information. The Apache Solr account name is dms. The password is hard-coded throughout the application, and is the same across all installations. Customers do not have the option to change passwords. The dms account for Apache Solr has access to all indexed patient documents.	2017-07-28	not yet calculated	CVE-2017-11694 MISC
medhost -- medhost	MEDHOST Document Management System contains hard-coded credentials that are used for customer database access. An attacker with knowledge of the hard-coded credentials and the ability to communicate directly with the database may be able to obtain or modify sensitive patient and financial information. PostgreSQL is used as the Document Management System	2017-07-28	not yet calculated	CVE-2017-11693 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	database. The account name is dms. The password is hard-coded throughout the application, and is the same across all installations. Customers do not have the option to change passwords. The dms account for PostgreSQL has access to the database schema for Document Management System.			
mediacoder -- mediacoder	Buffer overflow in MediaCoder 0.8.48.5888 allows remote attackers to execute arbitrary code via a crafted .m3u file.	2017-07-27	not yet calculated	CVE-2017-8869 EXPLOIT-DB(link is external)
mediawiki -- mediawiki	The MWOAuthDataStore::lookup_token function in Extension:OAuth for MediaWiki 1.25.x before 1.25.3, 1.24.x before 1.24.4, and before 1.23.11 does not properly validate the signature when checking the authorization signature, which allows remote registered Consumers to use another Consumer's credentials by leveraging knowledge of the credentials.	2017-07-25	not yet calculated	CVE-2015-8009 MLIST(link is external) CONFIRM
metinfo -- metinfo	job/uploadfile_save.php in MetInfo through 5.3.17 blocks the .php extension but not related extensions, which might allow remote authenticated admins to execute arbitrary PHP code by uploading a .phtml file after certain actions involving admin/system/safe.php and job/cv.php.	2017-07-28	not yet calculated	CVE-2017-11715 MISC(link is external)
metinfo -- metinfo	MetInfo through 5.3.17 allows stored XSS via HTML Edit Mode.	2017-07-28	not yet calculated	CVE-2017-11716 MISC(link is external)
metinfo -- metinfo	There is URL Redirector Abuse in MetInfo through 5.3.17 via the gourl parameter to member/login.php.	2017-07-28	not yet calculated	CVE-2017-11718 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
metinfo -- metinfo	MetInfo through 5.3.17 accepts the same CAPTCHA response for 120 seconds, which makes it easier for remote attackers to bypass intended challenge requirements by modifying the client-server data stream, as demonstrated by the login/findpass page.	2017-07-28	not yet calculated	CVE-2017-11717 MISC(link is external)
ming -- ming	A memory leak was found in the function parseSWF_SHAPEWITHSTYLE in util/parser.c in Ming 0.4.8, which allows attackers to cause a denial of service via a crafted file.	2017-07-28	not yet calculated	CVE-2017-11705 MISC(link is external) MISC(link is external)
ming -- ming	A memory leak vulnerability was found in the function parseSWF_DOACTION in util/parser.c in Ming 0.4.8, which allows attackers to cause a denial of service via a crafted file.	2017-07-28	not yet calculated	CVE-2017-11703 MISC(link is external) MISC(link is external)
ming -- ming	A heap-based buffer over-read was found in the function decompileIF in util/decompile.c in Ming 0.4.8, which allows attackers to cause a denial of service via a crafted file.	2017-07-28	not yet calculated	CVE-2017-11704 MISC(link is external) MISC(link is external)
mod_http2 -- mod_http2	A maliciously constructed HTTP/2 request could cause mod_http2 2.4.24, 2.4.25 to dereference a NULL pointer and crash the server process.	2017-07-26	not yet calculated	CVE-2017-7659 BID(link is external) SECTRACK(link is external) MLIST
mpg123 -- mpg123	The next_text function in src/libmpg123/id3.c in mpg123 1.24.0 allows remote attackers to cause a denial of service (buffer over-read) via a crafted mp3 file.	2017-07-27	not yet calculated	CVE-2017-9545 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
natapp -- oncommand_api_services	NetApp OnCommand API Services before 1.2P3 logs the LDAP BIND password when a user attempts to log in using the REST API, which allows remote authenticated users to obtain sensitive password information via unspecified vectors.	2017-07-25	not yet calculated	CVE-2017-8919 BID(link is external) CONFIRM (link is external)
netcomm -- wireless_routers	NetComm Wireless 4GT101W routers with Hardware: 0.01 / Software: V1.1.8.8 / Bootloader: 1.1.3 do not require authentication for logfile.html, status.html, or system_config.html.	2017-07-28	not yet calculated	CVE-2017-11645 MISC(link is external)
netcomm -- wireless_routers	NetComm Wireless 4GT101W routers with Hardware: 0.01 / Software: V1.1.8.8 / Bootloader: 1.1.3 are vulnerable to stored cross-site scripting attacks. Creating an SSID with an XSS payload results in successful exploitation.	2017-07-28	not yet calculated	CVE-2017-11647 MISC(link is external)
netcomm -- wireless_routers	NetComm Wireless 4GT101W routers with Hardware: 0.01 / Software: V1.1.8.8 / Bootloader: 1.1.3 are vulnerable to CSRF attacks, as demonstrated by using administration.html to disable the firewall. They does not contain any token that can mitigate CSRF vulnerabilities within the device.	2017-07-28	not yet calculated	CVE-2017-11646 MISC(link is external)
nexusphp -- nexusphp	NexusPHP V1.5 has XSS via a javascript: or data: URL in a UBBCode url tag.	2017-07-26	not yet calculated	CVE-2017-11651 MISC(link is external)
node.js -- node.js	Node.js v4.0 through v4.8.3, all versions of v5.x, v6.0 through v6.11.0, v7.0 through v7.10.0, and v8.0 through v8.1.3 was susceptible to hash flooding remote DoS attacks as the HashTable seed was constant across a given released version of Node.js. This was a result of building with V8 snapshots enabled by default which caused the initially randomized seed to be overwritten on startup.	2017-07-25	not yet calculated	CVE-2017-11499 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nss_compat_ossl -- nss_compat_ossl	The cipherstring parsing code in nss_compat_ossl while in multi-keyword mode does not match the expected set of ciphers for a given cipher combination, which allows attackers to have unspecified impact via unknown vectors.	2017-07-25	not yet calculated	CVE-2015-3278 CONFIRM (link is external)
ntp -- ntp	The "pidfile" or "driftfile" directives in NTP ntpd 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77, when ntpd is configured to allow remote configuration, allows remote attackers with an IP address that is allowed to send configuration requests, and with knowledge of the remote configuration password to write to arbitrary files via the :config command.	2017-07-24	not yet calculated	CVE-2015-7703 CONFIRM BID(link is external) CONFIRM (link is external) GENTOO
ntp -- ntp	The panic_gate check in NTP before 4.2.8p5 is only re-enabled after the first change to the system clock that was greater than 128 milliseconds by default, which allows remote attackers to set NTP to an arbitrary time when started with the -g option, or to alter the time by up to 900 seconds otherwise by responding to an unspecified number of requests from trusted sources, and leveraging a resulting denial of service (abort and restart).	2017-07-21	not yet calculated	CVE-2015-5300 CONFIRM (link is external) FEDORA FEDORA FEDORA SUSE SUSE SUSE SUSE SUSE SUSE SUSE SUSE REDHAT(link is external) MLIST CONFIRM CONFIRM DEBIAN CONFIRM (link is external) BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				SECTRAC K(link is external) UBUNTU(link is external) CONFIRM (link is external) CONFIRM (link is external) MISC CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) MISC(link is external) FREEBSD CONFIRM (link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				external) CONFIRM (link is external) CONFIRM (link is external)
nvidia -- windows_gpu_display_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer helper function where an incorrect calculation of string length may lead to denial of service.	2017-07-28	not yet calculated	CVE-2017-6260 CONFIRM (link is external)
nvidia -- windows_gpu_display_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer handler where a missing permissions check may allow users to gain access to arbitrary physical system memory, which may lead to an escalation of privileges.	2017-07-28	not yet calculated	CVE-2017-6251 CONFIRM (link is external)
nvidia -- windows_gpu_display_driver	NVIDIA GPU Display Driver contains a vulnerability in the kernel mode layer handler where a NULL pointer dereference may lead to denial of service or potential escalation of privileges	2017-07-28	not yet calculated	CVE-2017-6257 CONFIRM (link is external)
nvidia -- windows_gpu_display_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer handler where a NULL pointer dereference may lead to a denial of service or potential escalation of privileges.	2017-07-28	not yet calculated	CVE-2017-6252 CONFIRM (link is external)
nvidia -- windows_gpu_display_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where the size of an input buffer is not validated which may lead to denial of service or potential escalation of privileges	2017-07-28	not yet calculated	CVE-2017-6253 CONFIRM (link is external)
nvidia -- windows_gpu_display_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where an improper input	2017-07-28	not yet	CVE-2017-6255 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameter handling may lead to a denial of service or potential escalation of privileges.		calculated	(link is external)
nvidia -- windows_gpu_display_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where a value passed from a user to the driver is not correctly validated and used as the index to an array which may lead to denial of service or potential escalation of privileges.	2017-07-28	not yet calculated	CVE-2017-6256 CONFIRM (link is external)
nvidia -- windows_gpu_display_driver	NVIDIA GPU Display Driver contains a vulnerability in the kernel mode layer handler where an incorrect detection and recovery from an invalid state produced by specific user actions may lead to denial of service.	2017-07-28	not yet calculated	CVE-2017-6259 CONFIRM (link is external)
nvidia -- windows_gpu_display_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where a pointer passed from an user to the driver is used without validation which may lead to denial of service or potential escalation of privileges.	2017-07-28	not yet calculated	CVE-2017-6254 CONFIRM (link is external)
openjdk8 -- openjdk8	The Hotspot component in OpenJDK8 as packaged in Red Hat Enterprise Linux 6 and 7 allows local users to write to arbitrary files via a symlink attack.	2017-07-25	not yet calculated	CVE-2015-3149 REDHAT(link is external) BID(link is external) CONFIRM (link is external)
openpgp.js -- openpgp.js	s2k.js in OpenPGP.js will decrypt arbitrary messages regardless of passphrase for crafted PGP keys which allows remote attackers to bypass authentication if message decryption is used as an authentication mechanism via	2017-07-25	not yet calculated	CVE-2015-8013 MLIST(link is external) BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a crafted symmetrically encrypted PGP message.			CONFIRM (link is external)
openproject -- openproject	OpenProject before 6.1.6 and 7.x before 7.0.3 mishandles session expiry, which allows remote attackers to perform APIv3 requests indefinitely by leveraging a hijacked session.	2017-07-26	not yet calculated	CVE-2017-11667 CONFIRM (link is external) CONFIRM CONFIRM
oxide-qt -- oxide-qt	The oxide::JavaScriptDialogManager function in oxide-qt before 1.9.1 as packaged in Ubuntu 15.04 and Ubuntu 14.04 allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a crafted website.	2017-07-25	not yet calculated	CVE-2015-1332 CONFIRM (link is external) BID(link is external) UBUNTU(link is external) CONFIRM (link is external)
panda_security -- kernel_memory_access_driver	Heap-based buffer overflow in Panda Security Kernel Memory Access Driver 1.0.0.13 allows attackers to execute arbitrary code with kernel privileges via a crafted size input for allocated kernel paged pool and allocated non-paged pool buffers.	2017-07-25	not yet calculated	CVE-2015-1438 MISC(link is external) FULLDISC FULLDISC BID(link is external) MISC(link is external)
php -- php	In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, a stack-based buffer overflow in the zend_ini_do_op() function in Zend/zend_ini_parser.c could cause a denial of service or potentially allow executing code. NOTE: this is only	2017-07-25	not yet calculated	CVE-2017-11628 MISC(link is external) MISC(link

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	relevant for PHP applications that accept untrusted input (instead of the system's php.ini file) for the parse_ini_string or parse_ini_file function, e.g., a web application for syntax validation of php.ini directives.			is external) BID(link is external) MISC(link is external)
qemu -- qemu	The dhcp_decode function in slirp/bootp.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (out-of-bounds read and QEMU process crash) via a crafted DHCP options string.	2017-07-25	not yet calculated	CVE-2017-11434 MLIST(link is external) BID(link is external) CONFIRM (link is external) MLIST
qpdf -- qpdf	A stack-consumption vulnerability was found in libqpdf in QPDF 6.0.0, which allows attackers to cause a denial of service via a crafted file, related to the QPDFTokenizer::resolveLiteral function in QPDFTokenizer.cc after two consecutive calls to QPDFObjectHandle::parseInternal, aka an "infinite loop."	2017-07-25	not yet calculated	CVE-2017-11624 MISC(link is external) MISC(link is external)
qpdf -- qpdf	A stack-consumption vulnerability was found in libqpdf in QPDF 6.0.0, which allows attackers to cause a denial of service via a crafted file, related to the QPDFTokenizer::resolveLiteral function in QPDFTokenizer.cc after four consecutive calls to QPDFObjectHandle::parseInternal, aka an "infinite loop."	2017-07-25	not yet calculated	CVE-2017-11626 MISC(link is external) MISC(link is external)
qpdf -- qpdf	A stack-consumption vulnerability was found in libqpdf in QPDF 6.0.0, which allows attackers to cause a denial of service via a crafted file, related to the QPDF::resolveObjectsInStream function in QPDF.cc, aka an "infinite loop."	2017-07-25	not yet calculated	CVE-2017-11625 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC(link is external)
qpdf -- qpdf	A stack-consumption vulnerability was found in libqpdf in QPDF 6.0.0, which allows attackers to cause a denial of service via a crafted file, related to the PointerHolder function in PointerHolder.hh, aka an "infinite loop."	2017-07-25	not yet calculated	CVE-2017-11627 MISC(link is external) MISC(link is external)
quick_emulator -- quick_emulator	Heap-based buffer overflow in Cirrus CLGD 54xx VGA Emulator in Quick Emulator (Qemu) 2.8 and earlier allows local guest OS users to execute arbitrary code or cause a denial of service (crash) via vectors related to a VNC client updating its display after a VGA operation.	2017-07-25	not yet calculated	CVE-2017-7980 UBUNTU(link is external) MLIST(link is external) BID(link is external) CONFIRM(link is external) GENTOO
redhat -- arts_and_kdelibs	aRts 1.5.10 and kdelibs3 3.5.10 and earlier do not properly create temporary directories, which allows local users to hijack the IPC by pre-creating the temporary directory.	2017-07-25	not yet calculated	CVE-2015-7543 CONFIRM(link is external)
resiprocate -- resiprocate	The SdpContents::Session::Medium::parse function in resip/stack/SdpContents.cxx in reSIProcate 1.10.2 allows remote attackers to cause a denial of service (memory consumption) by triggering many media connections.	2017-07-22	not yet calculated	CVE-2017-11521 CONFIRM(link is external)
rsyslog -- rsyslog	rsyslog uses weak permissions for generating log files, which allows local users to obtain sensitive information by reading files in /var/log/cron.	2017-07-25	not yet calculated	CVE-2015-3243 MLIST(link is external) MLIST(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				external) BID(link is external) SECTRACK(link is external) CONFIRM (link is external)
sap -- netweaver	XML external entity (XXE) vulnerability in com.sap.km.cm.ice in SAP NetWeaver AS JAVA 7.5 allows remote authenticated users to read arbitrary files or conduct server-side request forgery (SSRF) attacks via a crafted DTD in an XML request, aka SAP Security Note 2387249.	2017-07-25	not yet calculated	CVE-2017-11457 MISC(link is external)
sap -- netweaver	Cross-site scripting (XSS) vulnerability in the ctcprotocol/Protocol servlet in SAP NetWeaver AS JAVA 7.3 allows remote attackers to inject arbitrary web script or HTML via the sessionID parameter, aka SAP Security Note 2406783.	2017-07-25	not yet calculated	CVE-2017-11458 MISC(link is external)
sap -- trex	SAP TREX 7.10 allows remote attackers to (1) read arbitrary files via an fget command or (2) write to arbitrary files and consequently execute arbitrary code via an fdir command, aka SAP Security Note 2419592.	2017-07-25	not yet calculated	CVE-2017-11459 MISC(link is external)
sendio -- sendio	Sendio versions before 8.2.1 were affected by a Local File Inclusion vulnerability that allowed an unauthenticated, remote attacker to read potentially sensitive system files via a specially crafted URL.	2017-07-27	not yet calculated	CVE-2016-10399 CONFIRM (link is external)
simplerisk -- simplerisk	In SimpleRisk 20170614-001, a CSRF attack on reset.php (aka the Send Password Reset Email form) can insert XSS sequences via the user parameter.	2017-07-24	not yet calculated	CVE-2017-10711 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC(link is external)
sipcrack -- sipcrack	An out-of-bounds read and write flaw was found in the way SIPcrack 0.2 processed SIP traffic, because 0x00 termination of a payload array was mishandled. A remote attacker could potentially use this flaw to crash the sipdump process by generating specially crafted SIP traffic.	2017-07-26	not yet calculated	CVE-2017-11654 MISC(link is external)
sipcrack -- sipcrack	A memory leak was found in the way SIPcrack 0.2 handled processing of SIP traffic, because a lines array was mismanaged. A remote attacker could potentially use this flaw to crash long-running sipdump network sniffing sessions.	2017-07-26	not yet calculated	CVE-2017-11655 MISC(link is external)
soundtouch -- soundtouch	The TDStretch::processSamples function in source/SoundTouch/TDStretch.cpp in SoundTouch 1.9.2 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted wav file.	2017-07-27	not yet calculated	CVE-2017-9258 MISC
soundtouch -- soundtouch	The TDStretchSSE::calcCrossCorr function in source/SoundTouch/sse_optimized.cpp in SoundTouch 1.9.2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted wav file.	2017-07-27	not yet calculated	CVE-2017-9260 MISC
soundtouch -- soundtouch	The TDStretch::acceptNewOverlapLength function in source/SoundTouch/TDStretch.cpp in SoundTouch 1.9.2 allows remote attackers to cause a denial of service (memory allocation error and application crash) via a crafted wav file.	2017-07-27	not yet calculated	CVE-2017-9259 MISC
statamic -- statamic_framework	Statamic framework before 2.6.0 does not correctly check a session's permissions when the methods from a	2017-07-24	not yet	CVE-2017-11422

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	user's class are called. Problematic methods include reset password, create new account, create new role, etc.		calculated	MISC(link is external)
synology -- synology_diskstation_manager	An information exposure vulnerability in forget_passwd.cgi in Synology DiskStation Manager (DSM) before 6.1.3-15152 allows remote attackers to enumerate valid usernames via unspecified vectors.	2017-07-24	not yet calculated	CVE-2017-9554 CONFIRM(link is external)
synology -- synology_diskstation_manager	A design flaw in SYNO.API.Encryption in Synology DiskStation Manager (DSM) before 6.1.3-15152 allows remote attackers to bypass the encryption protection mechanism via the crafted version parameter.	2017-07-24	not yet calculated	CVE-2017-9553 CONFIRM(link is external)
tilde -- tilde	An issue was discovered in Tilde CMS 1.0.1. Arbitrary files can be read via a file=../ attack on actionphp/download.File.php.	2017-07-24	not yet calculated	CVE-2017-11325 MISC
vmware -- vcenter_server	VMware vCenter Server 5.5, 6.0, 6.5 allows vSphere users with certain, limited vSphere privileges to use the VIX API to access Guest Operating Systems without the need to authenticate.	2017-07-28	not yet calculated	CVE-2017-4919 CONFIRM(link is external)
waves -- maxxaudio	Waves MaxxAudio, as installed on Dell laptops, adds a "WavesSysSvc" Windows service with File Version 1.1.6.0. This service has a vulnerability known as Unquoted Service Path. This could potentially allow an authorized but non-privileged local user to execute arbitrary code with elevated privileges on the system.	2017-07-26	not yet calculated	CVE-2017-6005 MISC(link is external)
wg-c10 -- wg-c10	WG-C10 v3.0.79 and earlier allows an attacker to bypass access restrictions to obtain or alter information stored in the external storage connected to the product via unspecified vectors.	2017-07-21	not yet calculated	CVE-2017-2277 MISC(link is external) JVN(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wildfly -- wildfly	The Undertow module of WildFly 9.x before 9.0.0.CR2 and 10.x before 10.0.0.Alpha1 allows remote attackers to obtain the source code of a JSP page via a "/" at the end of a URL.	2017-07-21	not yet calculated	CVE-2015-3198 CONFIRM (link is external) MISC CONFIRM MISC(link is external)
wmr-433 -- wmr-433	Cross-site request forgery (CSRF) vulnerability in WMR-433 firmware Ver.1.02 and earlier, WMR-433W firmware Ver.1.40 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2017-07-21	not yet calculated	CVE-2017-2273 CONFIRM (link is external) JVN(link is external)
wordpress -- wordpress	In the WP Rocket plugin 2.9.3 for WordPress, the Local File Inclusion mitigation technique is to trim traversal characters (..) -- however, this is insufficient to stop remote attacks and can be bypassed by using 0x00 bytes, as demonstrated by a .%00.../.%00.../ attack.	2017-07-26	not yet calculated	CVE-2017-11658 MISC(link is external) MISC(link is external)
wube -- factorio	A sandbox escape in the Lua interface in Wube Factorio before 0.15.31 allows remote game servers or user-assisted attackers to execute arbitrary C code by including and loading a C library.	2017-07-26	not yet calculated	CVE-2017-11615 MISC(link is external)
zencart -- zencart	The traverseStrictSanitize function in admin_dir/includes/classes/AdminRequestSanitizer.php in ZenCart 1.5.5e mishandles key strings, which allows remote authenticated users to execute arbitrary PHP code by placing that code into an invalid array index of the admin_name array parameter to admin_dir/login.php, if there is an export of an error-log entry for that invalid array index.	2017-07-27	not yet calculated	CVE-2017-11675 MISC(link is external)
zenphoto -- zenphoto	The sanitize_string function in ZenPhoto before 1.4.9 utilized the html_entity_decode function after input	2017-07-25	not yet	CVE-2015-5594 MISC(link

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sanitation, which might allow remote attackers to perform a cross-site scripting (XSS) via a crafted string.		calculated	is external) MLIST(link is external) CONFIRM MISC
zoho -- manageengine_event_log_analyzer	Zoho ManageEngine Event Log Analyzer 11.4 and 11.5 allows remote attackers to obtain an authenticated user's password via XSS vulnerabilities or sniffing non-SSL traffic on the network, because the password is represented in a cookie with a reversible encoding method.	2017-07-27	not yet calculated	CVE-2017-11686 MISC(link is external)
zoho -- manageengine_event_log_analyzer	Multiple Reflective cross-site scripting (XSS) vulnerabilities in search and display of event data in Zoho ManageEngine Event Log Analyzer 11.4 and 11.5 allow remote attackers to inject arbitrary web script or HTML, as demonstrated by the fName parameter.	2017-07-27	not yet calculated	CVE-2017-11685 MISC(link is external)
zoho -- manageengine_event_log_analyzer	Multiple Persistent cross-site scripting (XSS) vulnerabilities in Event log parsing and Display functions in Zoho ManageEngine Event Log Analyzer 11.4 and 11.5 allow remote attackers to inject arbitrary web script or HTML via syslog.	2017-07-27	not yet calculated	CVE-2017-11687 MISC(link is external)
zyxel -- zyxel	ZyXEL PK5001Z devices have zyad5001 as the su password, which makes it easier for remote attackers to obtain root access if a non-root account password is known (or a non-root default account exists within an ISP's deployment of these devices).	2017-07-25	not yet calculated	CVE-2016-10401 MISC