Vulnerability Summary for the Week of September 4, 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
ffmpeg -- ffmpeg	In libavformat/mxfdec.c in FFmpeg 3.3.3, a DoS in mxf_read_index_entry_array() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted MXF file, which claims a large "nb_index_entries" field in the header but does not contain sufficient backing data, is provided, the loop would consume huge CPU resources, since there is no EOF check inside the loop. Moreover, this big loop can be invoked multiple times if there is more than one applicable data segment in the crafted MXF file.	2017-09-07	7.1	CVE-2017-14170 CONFIRM(link is external)
ffmpeg -- ffmpeg	In libavformat/nsvdec.c in FFmpeg 3.3.3, a DoS in nsv_parse_NSVf_header() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted NSV file, which claims a large "table_entries_used" field in the header but does not contain sufficient backing data, is provided, the loop over 'table_entries_used' would consume huge CPU resources, since there is no EOF check inside the loop.	2017-09-07	7.1	CVE-2017-14171 CONFIRM(link is external)
fujixerox -- contentsbridge_utility	Untrusted search path vulnerability in Installer for ContentsBridge Utility for Windows 7.4.0 and earlier allows an attacker	2017-09-01	9.3	CVE-2017-10851 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to gain privileges via a Trojan horse DLL in an unspecified directory.			JVN(link is external)
fujixerox -- docuworks	Untrusted search path vulnerability in Installers for DocuWorks 8.0.7 and earlier and DocuWorks Viewer Light published in Jul 2017 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-09-01	9.3	CVE-2017-10848 CONFIRM(link is external) JVN(link is external)
fujixerox -- docuworks	Untrusted search path vulnerability in Self-extracting document generated by DocuWorks 8.0.7 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-09-01	9.3	CVE-2017-10849 CONFIRM(link is external) JVN(link is external)
gnome -- gedit	libgedit.a in GNOME gedit through 3.22.1 allows remote attackers to cause a denial of service (CPU consumption) via a file that begins with many '\0' characters.	2017-09-05	7.1	CVE-2017-14108 MISC(link is external) MISC(link is external)
helpdezk -- helpdezk	HelpDEZk 1.1.1 has SQL Injection in app\modules\admin\controllers\loginController.php via the admin/login/getWarningInfo/id/ PATH_INFO, related to the selectWarning function.	2017-09-05	7.5	CVE-2017-14145 MISC(link is external)
imagemagick -- imagemagick	The ReadOneLayer function in coders/xcf.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted file.	2017-09-01	7.1	CVE-2017-12691 CONFIRM(link is external)
imagemagick -- imagemagick	The ReadVIFFImage function in coders/viff.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted VIFF file.	2017-09-01	7.1	CVE-2017-12692 CONFIRM(link is external)
imagemagick -- imagemagick	The ReadBMPImage function in coders/bmp.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted BMP file.	2017-09-01	7.1	CVE-2017-12693 CONFIRM(link is external)
imagemagick -- imagemagick	ReadWEBPImage in coders/webp.c in ImageMagick 7.0.6-5 has an issue where memory allocation is excessive because it depends only on a length field in a header.	2017-09-04	7.5	CVE-2017-14137 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
imagemagick -- imagemagick	ImageMagick 7.0.6-5 has a memory leak vulnerability in ReadWEBPImage in coders/webp.c because memory is not freed in certain error cases, as demonstrated by VP8 errors.	2017-09-04	7.5	CVE-2017-14138 CONFIRM(link is external)
imagemagick -- imagemagick	In coders/ps.c in ImageMagick 7.0.7-0 Q16, a DoS in ReadPSImage() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted PSD file, which claims a large "extent" field in the header but does not contain sufficient backing data, is provided, the loop over "length" would consume huge CPU resources, since there is no EOF check inside the loop.	2017-09-07	7.1	CVE-2017-14172 CONFIRM(link is external) CONFIRM(link is external)
imagemagick -- imagemagick	In coders/psd.c in ImageMagick 7.0.7-0 Q16, a DoS in ReadPSDLayersInternal() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted PSD file, which claims a large "length" field in the header but does not contain sufficient backing data, is provided, the loop over "length" would consume huge CPU resources, since there is no EOF check inside the loop.	2017-09-07	7.1	CVE-2017-14174 CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)
imagemagick -- imagemagick	In coders/xbm.c in ImageMagick 7.0.6-1 Q16, a DoS in ReadXBMImage() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted XBM file, which claims large rows and columns fields in the header but does not contain sufficient backing data, is provided, the loop over the rows would consume huge CPU resources, since there is no EOF check inside the loop.	2017-09-07	7.1	CVE-2017-14175 CONFIRM(link is external) CONFIRM(link is external)
mcafee -- security_scan_plus	A Code Injection vulnerability in the non-certificate-based authentication mechanism in McAfee Live Safe versions prior to 16.0.3 and McAfee Security Scan Plus (MSS+) versions prior to 3.11.599.3 allows network attackers to perform a malicious file execution via a HTTP backend-response.	2017-09-01	7.5	CVE-2017-3897 CONFIRM(link is external) BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netapp -- data_ontap	NetApp Data ONTAP before 8.2.4, when operating in 7-Mode, allows remote attackers to bypass authentication and (1) obtain sensitive information from or (2) modify volumes via vectors related to UTF-8 in the volume language.	2017-09-01	7.5	CVE-2015-7746 CONFIRM(link is external)
ntt -- enkaku_support_tool	Untrusted search path vulnerability in Remote Support Tool (Enkaku Support Tool) All versions distributed through the website till 2017 August 10 allow an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-09-01	9.3	CVE-2017-10829 CONFIRM(link is external) MISC(link is external) JVN(link is external)
rarlab -- unrar	unrar 0.0.1 (aka unrar-free or unrar-gpl) suffers from a stack-based buffer over-read in unrarlib.c, related to ExtrFile and stricomp.	2017-09-03	7.5	CVE-2017-14122 MISC(link is external) MISC
salesagility -- suitecrm	Race condition in SuiteCRM before 7.2.3 allows remote attackers to execute arbitrary code. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-5947.	2017-09-06	9.3	CVE-2015-5948 MLIST(link is external) MISC(link is external) CONFIRM(link is external) CONFIRM(link is external)
sap -- netweaver	XML External Entity (XXE) vulnerability in SAP Netweaver before 7.01.	2017-09-06	7.5	CVE-2015-7241 MISC(link is external) BUGTRAQ(link is external) BID(link is external) EXPLOIT-DB(link is external)
scrapy -- scrapy	Scrapy 1.4 allows remote attackers to cause a denial of service (memory consumption) via	2017-09-05	7.8	CVE-2017-14158

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	large files because arbitrarily many files are read into memory, which is especially problematic if the files are then individually written in a separate thread to a slow storage resource, as demonstrated by interaction between dataReceived (in core/downloader/handlers/http11.py) and S3FilesStore.			MISC(link is external) MISC(link is external)
simplesamlphp -- simplesamlphp	The secureCompare method in lib/SimpleSAML/Utils/Crypto.php in SimpleSAMLphp 1.14.13 and earlier, when used with PHP before 5.6, allows attackers to conduct session fixation attacks or possibly bypass authentication by leveraging missing character conversions before an XOR operation.	2017-09-01	7.5	CVE-2017-12868 CONFIRM(link is external) CONFIRM
simplesamlphp -- simplesamlphp	SimpleSAMLphp 1.7.0 through 1.14.10 might allow attackers to obtain sensitive information, gain unauthorized access, or have unspecified other impacts by leveraging incorrect persistent NameID generation when an Identity Provider (IdP) is misconfigured.	2017-09-01	7.5	CVE-2017-12873 CONFIRM(link is external) CONFIRM
technicolor -- td5336_firmware	Command Injection in the Ping Module in the Web Interface on Technicolor TD5336 OI_Fw_v7 devices allows remote attackers to execute arbitrary OS commands as root via shell metacharacters in the pingAddr parameter to mnt_ping.cgi.	2017-09-04	10.0	CVE-2017-14127 MISC(link is external)

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aspl -- libaxl	Heap-based buffer overflow in libaxl 0.6.9 allows attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted XML document.	2017-09-06	6.8	CVE-2015-3450 MLIST(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				BID(link is external)
beaker-project -- beaker	XML external entity (XXE) vulnerability in bkr/server/jobs.py in Beaker before 20.1 allows remote authenticated users to obtain sensitive information via submitting job XML to the server containing entity references which reference files from the Beaker server's file system.	2017-09-06	4.0	CVE-2015-3160 MLIST(link is external) BID(link is external) CONFIRM CONFIRM (link is external) CONFIRM (link is external)
beaker-project -- beaker	The admin pages for power types and key types in Beaker before 20.1 do not have any access controls, which allows remote authenticated users to modify power types and key types via navigating to $BEAKER/powertypes and $BEAKER/keytypes respectively.	2017-09-06	4.0	CVE-2015-3163 MLIST(link is external) BID(link is external) CONFIRM CONFIRM (link is external)
bento4 -- bento4	The AP4_AtomSampleTable::GetSample function in Core/Ap4AtomSampleTable.cpp in Bento4 mp42ts before 1.5.0-616 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted mp4 file.	2017-09-06	4.3	CVE-2017-12474 MISC(link is external) MISC(link is external) MISC(link is external)
bento4 -- bento4	The AP4_Processor::Process function in Core/Ap4Processor.cpp in Bento4 mp4encrypt before 1.5.0-616 allows remote	2017-09-06	4.3	CVE-2017-12475 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted mp4 file.			MISC(link is external) MISC(link is external)
bento4 -- bento4	The AP4_AvccAtom::InspectFields function in Core/Ap4AvccAtom.cpp in Bento4 mp4dump before 1.5.0-616 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted mp4 file.	2017-09-06	4.3	CVE-2017-12476 MISC(link is external) MISC(link is external) MISC(link is external)
embedthis -- goahead	GoAhead 3.4.0 through 3.6.5 has a NULL Pointer Dereference in the websDecodeUrl function in http.c, leading to a crash for a "POST / HTTP/1.1" request.	2017-09-05	5.0	CVE-2017-14149 MISC(link is external)
eyesofnetwork -- eonweb	In the EyesOfNetwork web interface (aka eonweb) 5.1-0, module\tool_all\tools\interface.php does not properly restrict exec calls, which allows remote attackers to execute arbitrary commands via shell metacharacters in the host_list parameter to module/tool_all/select_tool.php.	2017-09-03	6.5	CVE-2017-14118 MISC
eyesofnetwork -- eonweb	In the EyesOfNetwork web interface (aka eonweb) 5.1-0, module\tool_all\tools\snmpwalk.php does not properly restrict popen calls, which allows remote attackers to execute arbitrary commands via shell metacharacters in a parameter.	2017-09-03	6.5	CVE-2017-14119 MISC
ffmpeg -- ffmpeg	In the mxf_read_primer_pack function in libavformat/mxfdec.c in	2017-09-07	6.8	CVE-2017-14169

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	FFmpeg 3.3.3, an integer signedness error might occur when a crafted file, which claims a large "item_num" field such as 0xffffffff, is provided. As a result, the variable "item_num" turns negative, bypassing the check for a large value.			CONFIRM (link is external)
froxlor -- froxlor	Froxlor before 0.9.33.2 with the default configuration/setup might allow remote attackers to obtain the database password by reading /logs/sql-error.log.	2017-09-06	5.0	CVE-2015-5959 MLIST(link is external) BID(link is external) CONFIRM (link is external)
gnome -- evince	backend/comics/comics-document.c (aka the comic book backend) in GNOME Evince before 3.24.1 allows remote attackers to execute arbitrary commands via a .cbt file that is a TAR archive containing a filename beginning with a "--" command-line option substring, as demonstrated by a --checkpoint-action=exec=bash at the beginning of the filename.	2017-09-05	6.8	CVE-2017-1000083 MISC BID(link is external) MISC MISC(link is external)
gnome -- gdk-pixbuf	An exploitable heap overflow vulnerability exists in the gdk_pixbuf__jpeg_image_load_increment functionality of Gdk-Pixbuf 2.36.6. A specially crafted jpeg file can cause a heap overflow resulting in remote code execution. An	2017-09-05	6.8	CVE-2017-2862 BID(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker can send a file or url to trigger this vulnerability.			
gnome -- gdk-pixbuf	An exploitable integer overflow vulnerability exists in the tiff_image_parse functionality of Gdk-Pixbuf 2.36.6 when compiled with Clang. A specially crafted tiff file can cause a heap-overflow resulting in remote code execution. An attacker can send a file or a URL to trigger this vulnerability.	2017-09-05	6.8	CVE-2017-2870 BID(link is external) MISC(link is external)
gnu -- binutils	The decode_line_info function in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (read_1_byte heap-based buffer over-read and application crash) via a crafted ELF file.	2017-09-04	4.3	CVE-2017-14128 BID(link is external) CONFIRM CONFIRM
gnu -- binutils	The read_section function in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (parse_comp_unit heap-based buffer over-read and application crash) via a crafted ELF file.	2017-09-04	4.3	CVE-2017-14129 BID(link is external) CONFIRM CONFIRM
gnu -- binutils	The _bfd_elf_parse_attributes function in elf-attrs.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (_bfd_elf_attr_strdup heap-based buffer over-read and	2017-09-04	4.3	CVE-2017-14130 BID(link is external) CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	application crash) via a crafted ELF file.			
graphicsmagick -- graphicsmagick	The ReadJNGImage and ReadOneJNGImage functions in coders/png.c in GraphicsMagick 1.3.26 do not properly manage image pointers after certain error conditions, which allows remote attackers to conduct use-after-free attacks via a crafted file, related to a ReadMNGImage out-of-order CloseBlob call. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-11403.	2017-09-01	6.8	CVE-2017-14103 MISC(link is external) MISC
helpdezk -- helpdezk	HelpDEZk 1.1.1 allows remote authenticated users to execute arbitrary PHP code by uploading a .php attachment and then requesting it in the helpdezk\app\uploads\helpdezk\attachments\ directory.	2017-09-05	6.5	CVE-2017-14146 MISC(link is external)
honda -- moto_linc	Honda Moto LINC 1.6.1 does not verify SSL certificates.	2017-09-06	4.3	CVE-2015-2943 JVN(link is external) JVNDB(link is external)
ibm -- emptoris_strategic_supply_management	IBM Emptoris Strategic Supply Management Platform 10.0.0.x through 10.1.1.x is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 120657.	2017-09-05	6.8	CVE-2017-1097 CONFIRM(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- inotes	IBM Notes 8.5 and 9.0 is vulnerable to a denial of service. If a user is persuaded to click on a malicious link, it could cause the Notes client to hang and have to be restarted. IBM X-Force ID: 121370.	2017-09-05	4.3	CVE-2017-1129 CONFIRM (link is external) CONFIRM (link is external) MISC(link is external) EXPLOIT-DB(link is external)
ibm -- inotes	IBM Notes 8.5 and 9.0 is vulnerable to a denial of service. If a user is persuaded to click on a malicious link, it would open up many file select dialog boxes which would cause the client hang and have to be restarted. IBM X-Force ID: 121371.	2017-09-05	4.3	CVE-2017-1130 CONFIRM (link is external) BID(link is external) MISC(link is external) EXPLOIT-DB(link is external)
ibm -- qradar_network_security	IBM QRadar Network Security 5.4 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: 128376.	2017-09-05	4.3	CVE-2017-1457 CONFIRM (link is external) BID(link is external) MISC(link is external)
ibm -- qradar_network_security	IBM QRadar Network Security 5.4 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability	2017-09-05	5.5	CVE-2017-1458 CONFIRM (link is external) BID(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to expose sensitive information or consume memory resources. IBM X-Force ID: 128377.			external) MISC(link is external)
ibm -- qradar_network_security	IBM QRadar Network Security 5.4 supports interaction between multiple actors and allows those actors to negotiate which algorithm should be used as a protection mechanism such as encryption or authentication, but it does not select the strongest algorithm that is available to both parties. IBM X-Force ID: 128689.	2017-09-05	5.0	CVE-2017-1491 CONFIRM (link is external) MISC(link is external)
imagemagick -- imagemagick	ImageMagick 7.0.6-2 has a memory leak vulnerability in WriteMSLImage in coders/msl.c.	2017-09-04	6.8	CVE-2017-14139 CONFIRM (link is external)
imagemagick -- imagemagick	In the function ReadTXTImage() in coders/txt.c in ImageMagick 7.0.6-10, an integer overflow might occur for the addition operation "GetQuantumRange(depth)+1" when "depth" is large, producing a smaller value than expected. As a result, an infinite loop would occur for a crafted TXT file that claims a very large "max_value" value.	2017-09-07	4.3	CVE-2017-14173 CONFIRM (link is external) CONFIRM (link is external)
jasper_project -- jasper	JasPer 2.0.13 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted image, related to the jas_image_ishomosamp function in libjasper/base/jas_image.c.	2017-09-04	4.3	CVE-2017-14132 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ledger-cli -- ledger	An exploitable buffer overflow vulnerability exists in the tag parsing functionality of Ledger-CLI 3.1.1. A specially crafted journal file can cause an integer underflow resulting in code execution. An attacker can construct a malicious journal file to trigger this vulnerability.	2017-09-05	6.8	CVE-2017-2807 BID(link is external) MISC(link is external)
ledger-cli -- ledger	An exploitable use-after-free vulnerability exists in the account parsing component of the Ledger-CLI 3.1.1. A specially crafted ledger file can cause a use-after-free vulnerability resulting in arbitrary code execution. An attacker can convince a user to load a journal file to trigger this vulnerability.	2017-09-05	6.8	CVE-2017-2808 BID(link is external) MISC(link is external)
lexmark -- perceptive_document_filters	An exploitable use-after-free exists in the PDF parsing functionality of Lexmark Perspective Document Filters 11.3.0.2400 and 11.4.0.2452. A crafted PDF document can lead to a use-after-free resulting in direct code execution.	2017-09-05	6.8	CVE-2017-2821 BID(link is external) MISC(link is external)
lexmark -- perceptive_document_filters	An exploitable code execution vulnerability exists in the image rendering functionality of Lexmark Perceptive Document Filters 11.3.0.2400. A specifically crafted PDF can cause a function call on a corrupted DCTStream to occur, resulting in user controlled data being written to the stack. A maliciously crafted PDF file can be used to trigger this vulnerability.	2017-09-05	6.8	CVE-2017-2822 BID(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
libarchive -- libarchive	libarchive 3.3.2 allows remote attackers to cause a denial of service (xml_data heap-based buffer over-read and application crash) via a crafted xar archive, related to the mishandling of empty strings in the atol8 function in archive_read_support_format_xar.c.	2017-09-06	4.3	CVE-2017-14166 MISC MISC(link is external)
libzip_project -- libzip	The _zip_read_eocd64 function in zip_open.c in libzip before 1.3.0 mishandles EOCD records, which allows remote attackers to cause a denial of service (memory allocation failure in _zip_cdir_grow in zip_dirent.c) via a crafted ZIP archive.	2017-09-01	4.3	CVE-2017-14107 MISC MISC(link is external)
linux -- linux_kernel	The tcp_disconnect function in net/ipv4/tcp.c in the Linux kernel before 4.12 allows local users to cause a denial of service (__tcp_select_window divide-by-zero error and system crash) by triggering a disconnect within a certain tcp_recvmsg code path.	2017-09-01	4.9	CVE-2017-14106 CONFIRM CONFIRM (link is external) CONFIRM
mcafee -- livesafe	A man-in-the-middle attack vulnerability in the non-certificate-based authentication mechanism in McAfee LiveSafe (MLS) versions prior to 16.0.3 allows network attackers to modify the Windows registry value associated with the McAfee update via the HTTP backend-response.	2017-09-01	4.3	CVE-2017-3898 CONFIRM (link is external)
mimedefang -- mimedefang	MIMEDefang 2.80 and earlier creates a PID file after dropping privileges to a non-	2017-09-01	4.6	CVE-2017-14102

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill `cat /pathname`" command, as demonstrated by the init-script.in and mimedefang-init.in scripts.			MISC(link is external) MISC(link is external)
netapp -- clustered_data_ontap	NetApp Clustered Data ONTAP 8.3.x before 8.3.2P12 allows remote authenticated users to execute arbitrary code on the storage controller via unspecified vectors.	2017-09-01	6.5	CVE-2017-12421 CONFIRM (link is external)
netapp -- clustered_data_ontap	NetApp Clustered Data ONTAP 8.3.x before 8.3.2P12 allows remote authenticated users to read data on other Storage Virtual Machines (SVMs) via unspecified vectors.	2017-09-01	4.0	CVE-2017-12423 CONFIRM (link is external)
netapp -- data_ontap	NetApp Data ONTAP before 8.2.5 and 8.3.x before 8.3.2P12 allow remote authenticated users to cause a denial of service via vectors related to unsafe user input string handling.	2017-09-01	4.0	CVE-2016-1895 CONFIRM (link is external)
netapp -- oncommand_unified_manager_for_clustered_data_ontap	NetApp OnCommand Unified Manager for Clustered Data ONTAP before 7.2P1 does not set the secure flag for an unspecified cookie in an HTTPS session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an HTTP session.	2017-09-01	5.0	CVE-2017-14053 CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
opencv -- opencv	OpenCV (Open Source Computer Vision Library) 3.3 has an out-of-bounds write error in the function FillColorRow1 in utils.cpp when reading an image file by using cv::imread. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-12597.	2017-09-04	4.3	CVE-2017-14136 MISC(link is external) MISC(link is external) MISC(link is external)
openjpeg -- openjpeg	An off-by-one error was discovered in opj_tcd_code_block_enc_allocate_data in lib/openjp2/tcd.c in OpenJPEG 2.2.0. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service (heap-based buffer overflow affecting opj_mqc_flush in lib/openjp2/mqc.c and opj_t1_encode_cblk in lib/openjp2/t1.c) or possibly remote code execution.	2017-09-05	6.8	CVE-2017-14151 BID(link is external) MISC MISC(link is external) MISC(link is external)
openjpeg -- openjpeg	A mishandled zero case was discovered in opj_j2k_set_cinema_parameters in lib/openjp2/j2k.c in OpenJPEG 2.2.0. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service (heap-based buffer overflow affecting opj_write_bytes_LE in lib/openjp2/cio.c and opj_j2k_write_sot in lib/openjp2/j2k.c) or possibly remote code execution.	2017-09-05	6.8	CVE-2017-14152 MISC MISC(link is external) MISC(link is external)
qemu -- qemu	Use-after-free vulnerability in the sofree function in slirp/socket.c in QEMU (aka Quick Emulator) allows	2017-09-01	5.0	CVE-2017-13711 MLIST(lin

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to cause a denial of service (QEMU instance crash) by leveraging failure to properly clear ifq_so from pending packets.			k is external) BID(link is external) CONFIRM (link is external) MLIST
rarlab -- unrar	unrar 0.0.1 (aka unrar-free or unrar-gpl) suffers from a directory traversal vulnerability for RAR v2 archives: pathnames of the form ../[filename] are unpacked into the upper directory.	2017-09-03	5.0	CVE-2017-14120 MISC(link is external) MISC
rarlab -- unrar	The DecodeNumber function in unrarlib.c in unrar 0.0.1 (aka unrar-free or unrar-gpl) suffers from a NULL pointer dereference flaw triggered by a specially crafted RAR archive.	2017-09-03	6.8	CVE-2017-14121 MISC(link is external) MISC
simplesamlphp -- infocard_module	The InfoCard module 1.0 for SimpleSAMLphp allows attackers to spoof XML messages by leveraging an incorrect check of return values in signature validation utilities.	2017-09-01	5.0	CVE-2017-12874 CONFIRM
simplesamlphp -- simplesamlphp	The multiauth module in SimpleSAMLphp 1.14.13 and earlier allows remote attackers to bypass authentication context restrictions and use an authentication source defined in config/authsources.php via vectors related to improper validation of user input.	2017-09-01	5.0	CVE-2017-12869 CONFIRM
simplesamlphp -- simplesamlphp	SimpleSAMLphp 1.14.12 and earlier make it easier for man-in-the-middle attackers to obtain sensitive information by leveraging use of the aesEncrypt and aesDecrypt	2017-09-01	4.3	CVE-2017-12870 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	methods in the SimpleSAML/Utils/Crypto class to protect session identifiers in replies to non-HTTPS service providers.			
simplesamlphp -- simplesamlphp	The aesEncrypt method in lib/SimpleSAML/Utils/Crypto.php in SimpleSAMLphp 1.14.x through 1.14.11 makes it easier for context-dependent attackers to bypass the encryption protection mechanism by leveraging use of the first 16 bytes of the secret key as the initialization vector (IV).	2017-09-01	4.3	CVE-2017-12871 CONFIRM (link is external) CONFIRM
simplesamlphp -- simplesamlphp	The (1) Htpasswd authentication source in the authcrypt module and (2) SimpleSAML_Session class in SimpleSAMLphp 1.14.11 and earlier allow remote attackers to conduct timing side-channel attacks by leveraging use of the standard comparison operator to compare secret material against user input.	2017-09-01	4.3	CVE-2017-12872 CONFIRM
suitecrm -- suitecrm	SuiteCRM before 7.2.3 allows remote attackers to execute arbitrary code.	2017-09-06	6.8	CVE-2015-5947 MLIST(link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
vulcanjs -- vulcan	TelescopeJS before 0.15 leaks user bcrypt password hashes in	2017-09-06	5.0	CVE-2015-3454

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	websocket messages, which might allow remote attackers to obtain password hashes via a cross-site scripting attack.			MLIST(link is external) BID(link is external) CONFIRM(link is external) MISC(link is external)
xnau -- participants_database	The Participants Database plugin before 1.7.5.10 for WordPress has XSS.	2017-09-04	4.3	CVE-2017-14126 MISC(link is external) CONFIRM EXPLOIT-DB(link is external)

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
beaker-project -- beaker	The search bar code in bkr/server/widgets.py in Beaker before 20.1 does not escape </script> tags in string literals when producing JSON.	2017-09-06	3.5	CVE-2015-3161 MLIST(link is external) BID(link is external) CONFIRM MISC(link is external) CONFIRM(link is external)
beaker-project -- beaker	Cross-site scripting (XSS) vulnerability in the edit comment dialog in bkr/server/widgets.py in Beaker 20.1 allows remote authenticated users to inject arbitrary web script or HTML via writing a crafted comment on an acked or nacked cancelled job.	2017-09-06	3.5	CVE-2015-3162 MLIST(link is external) BID(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC(link is external) CONFIRM(link is external)
linux -- linux_kernel	The move_pages system call in mm/migrate.c in the Linux kernel before 4.12.9 doesn't check the effective uid of the target process, enabling a local attacker to learn the memory layout of a setuid executable despite ASLR.	2017-09-05	2.1	CVE-2017-14140 CONFIRM CONFIRM CONFIRM(link is external)
linux -- linux_kernel	The atyfb_ioctl function in drivers/video/fbdev/aty/atyfb_base.c in the Linux kernel through 4.12.10 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory by reading locations associated with padding bytes.	2017-09-05	2.1	CVE-2017-14156 BID(link is external) MISC(link is external) MISC(link is external) MISC(link is external)
qemu -- qemu	QEMU (aka Quick Emulator), when built with the VGA display emulator support, allows local guest OS privileged users to cause a denial of service (out-of-bounds read and QEMU process crash) via vectors involving display update.	2017-09-01	2.1	CVE-2017-13672 MLIST(link is external) BID(link is external) CONFIRM(link is external) MLIST

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
anchor-cms -- anchor-cms	Cross-site scripting (XSS) vulnerability in anchor-cms before 0.9-dev.	2017-09-07	not yet calculated	CVE-2015-5060 CONFIRM (link is external)
apache -- hadoop	The YARN NodeManager in Apache Hadoop 2.6.x before 2.6.5 and 2.7.x	2017-09-05	not yet	CVE-2016-3086

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	before 2.7.3 can leak the password for credential store provider used by the NodeManager to YARN Applications.		calculated	MLIST BID(link is external)
apache_directory -- ldap_api	Apache Directory LDAP API before 1.0.0-M31 allows attackers to conduct timing attacks via unspecified vectors.	2017-09-07	not yet calculated	CVE-2015-3250 CONFIRM MLIST(link is external) MLIST(link is external) CONFIRM (link is external)
askbot -- askbot	Cross-site scripting (XSS) vulnerability in askbot 0.7.51-4.el6.noarch.	2017-09-07	not yet calculated	CVE-2015-3169 MLIST(link is external) BID(link is external) CONFIRM (link is external)
asterisk -- asterisk	In Asterisk 11.x before 11.25.2, 13.x before 13.17.1, and 14.x before 14.6.1 and Certified Asterisk 11.x before 11.6-cert17 and 13.x before 13.13-cert5, unauthorized command execution is possible. The app_minivm module has an "externnotify" program configuration option that is executed by the MinivmNotify dialplan application. The application uses the caller-id name and number as part of a built string passed to the OS shell for interpretation and execution. Since the caller-id name and number can come from an untrusted source, a crafted caller-id name or number	2017-09-02	not yet calculated	CVE-2017-14100 CONFIRM SECTRAC K(link is external) CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows an arbitrary shell command injection.			
asterisk -- asterisk	In the pjsip channel driver (res_pjsip) in Asterisk 13.x before 13.17.1 and 14.x before 14.6.1, a carefully crafted tel URI in a From, To, or Contact header could cause Asterisk to crash.	2017-09-02	not yet calculated	CVE-2017-14098 CONFIRM BID(link is external) SECTRAC K(link is external) CONFIRM CONFIRM
asterisk -- asterisk	In res/res_rtp_asterisk.c in Asterisk 11.x before 11.25.2, 13.x before 13.17.1, and 14.x before 14.6.1 and Certified Asterisk 11.x before 11.6-cert17 and 13.x before 13.13-cert5, unauthorized data disclosure (media takeover in the RTP stack) is possible with careful timing by an attacker. The "strictrtp" option in rtp.conf enables a feature of the RTP stack that learns the source address of media for a session and drops any packets that do not originate from the expected address. This option is enabled by default in Asterisk 11 and above. The "nat" and "rtp_symmetric" options (for chan_sip and chan_pjsip, respectively) enable symmetric RTP support in the RTP stack. This uses the source address of incoming media as the target address of any sent media. This option is not enabled by default, but is commonly enabled to handle devices behind NAT. A change was made to the strict RTP support in the RTP stack to better tolerate late media when a reinvite occurs. When combined with the symmetric RTP support, this introduced an avenue where media could be hijacked. Instead of only	2017-09-02	not yet calculated	CVE-2017-14099 CONFIRM SECTRAC K(link is external) CONFIRM CONFIRM MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	learning a new address when expected, the new code allowed a new source address to be learned at all times. If a flood of RTP traffic was received, the strict RTP support would allow the new address to provide media, and (with symmetric RTP enabled) outgoing traffic would be sent to this new address, allowing the media to be hijacked. Provided the attacker continued to send traffic, they would continue to receive traffic as well.			
at&t -- u-verse_firmware	The AT&T U-verse 9.2.2h0d83 firmware for the Arris NVG589, NVG599, and unspecified other devices, when IP Passthrough mode is not used, configures an sbdc.ha WAN TCP service on port 61001 with the bdctest account and the bdctest password, which allows remote attackers to obtain sensitive information (such as the Wi-Fi password) by leveraging knowledge of a hardware identifier, related to the Bulk Data Collection (BDC) mechanism defined in Broadband Forum technical reports.	2017-09-03	not yet calculated	CVE-2017-10793 BID(link is external) MISC(link is external) MISC(link is external)
at&t -- u-verse_firmware	The AT&T U-verse 9.2.2h0d83 firmware for the Arris NVG599 device, when IP Passthrough mode is not used, configures WAN access to a caserver https service with the tech account and an empty password, which allows remote attackers to obtain root privileges by establishing a session on port 49955 and then installing new software, such as BusyBox with "nc -l" support.	2017-09-03	not yet calculated	CVE-2017-14116 BID(link is external) MISC(link is external) MISC(link is external)
at&t -- u-verse_firmware	The AT&T U-verse 9.2.2h0d83 firmware for the Arris NVG589 and NVG599 devices, when IP Passthrough mode is not used, configures ssh-permanent-enable	2017-09-03	not yet calculated	CVE-2017-14115 BID(link is external) MISC(link

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WAN SSH logins to the remotessh account with the 5SaP9I26 password, which allows remote attackers to access a "Terminal shell v1.0" service, and subsequently obtain unrestricted root privileges, by establishing an SSH session and then entering certain shell metacharacters and BusyBox commands.			is external) MISC(link is external)
at&t -- u-verse_firmware	The AT&T U-verse 9.2.2h0d83 firmware for the Arris NVG589 and NVG599 devices, when IP Passthrough mode is not used, configures an unauthenticated proxy service on WAN TCP port 49152, which allows remote attackers to establish arbitrary TCP connections to intranet hosts by sending \x2a\xce\x01 followed by other predictable values.	2017-09-03	not yet calculated	CVE-2017-14117 BID(link is external) MISC(link is external) MISC(link is external)
azeotech -- daqfactory	An Uncontrolled Search Path Element issue was discovered in AzeoTech DAQFactory versions prior to 17.1. An uncontrolled search path element vulnerability has been identified, which may execute malicious DLL files that have been placed within the search path.	2017-09-08	not yet calculated	CVE-2017-5147 BID(link is external) MISC
azeotech -- daqfactory	An Incorrect Default Permissions issue was discovered in AzeoTech DAQFactory versions prior to 17.1. Local, non-administrative users may be able to replace or modify original application files with malicious ones.	2017-09-08	not yet calculated	CVE-2017-12699 BID(link is external) MISC
centreon -- centreon	Cross-site scripting (XSS) vulnerability in Centreon 2.6.1.	2017-09-07	not yet calculated	CVE-2015-7672 MISC(link is external)
cisco -- asyncos_software_for_cisco_security_appliances	A vulnerability in the malware detection functionality within Advanced Malware Protection (AMP) of Cisco AsyncOS Software for Cisco Email Security Appliances (ESAs) could allow an	2017-09-07	not yet calculated	CVE-2017-12218 SECTRACK(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthenticated, remote attacker to cause an email attachment containing malware to be delivered to the end user. The vulnerability is due to the failure of AMP to scan certain EML attachments that could contain malware. An attacker could exploit this vulnerability by sending an email with a crafted EML attachment through the targeted device. A successful exploit could allow the attacker to bypass the configured ESA email message and content filtering and allow the malware to be delivered to the end user. Vulnerable Products: This vulnerability affects Cisco AsyncOS Software for Cisco ESA, both virtual and hardware appliances, that are configured with message or content filters to scan incoming email attachments on the ESA. Cisco Bug IDs: CSCuz81533.			(link is external)
cisco -- emergency_responder	A vulnerability in the SQL database interface for Cisco Emergency Responder could allow an authenticated, remote attacker to conduct a blind SQL injection attack. The vulnerability is due to a failure to validate user-supplied input used in SQL queries that bypass protection filters. An attacker could exploit this vulnerability by sending crafted URLs that include SQL statements. An exploit could allow the attacker to view or modify entries in some database tables, affecting the integrity of the data. Cisco Bug IDs: CSCvb58973.	2017-09-07	not yet calculated	CVE-2017-12227 BID(link is external) SECTRAC K(link is external) CONFIRM (link is external)
cisco -- firepower_management_center	A vulnerability in the web-based management interface of Cisco Firepower Management Center could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a	2017-09-07	not yet calculated	CVE-2017-12220 BID(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. Cisco Bug IDs: CSCvc50771.			(link is external)
cisco -- firepower_management_center	A vulnerability in the web framework of Cisco Firepower Management Center could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web interface of the affected software. The vulnerability is due to insufficient validation of user-supplied input by the affected software. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code in the context of the affected system. Cisco Bug IDs: CSCvc38983.	2017-09-07	not yet calculated	CVE-2017-12221 BID(link is external) CONFIRM (link is external)
cisco -- gprs_tunneling_protocol	A vulnerability in the General Packet Radio Service (GPRS) Tunneling Protocol ingress packet handler of Cisco ASR 5500 System Architecture Evolution (SAE) Gateways could allow an unauthenticated, remote attacker to cause a partial denial of service (DoS) condition on an affected device. The vulnerability is due to improper input validation of GPRS Tunneling Protocol packet headers. An attacker could exploit this vulnerability by sending a malformed	2017-09-07	not yet calculated	CVE-2017-12217 BID(link is external) SECTRACK(link is external) CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	GPRS Tunneling Protocol packet to an affected device. A successful exploit could allow the attacker to cause the GTPUMGR process on an affected device to restart unexpectedly, resulting in a partial DoS condition. If the GTPUMGR process restarts, there could be a brief impact on traffic passing through the device. Cisco Bug IDs: CSCve07119.			
cisco -- ios_and_ios_xe	A vulnerability in the IPv6 Simple Network Management Protocol (SNMP) code of Cisco IOS and Cisco IOS XE Software could allow an authenticated, remote attacker to cause high CPU usage or a reload of the device. The vulnerability is due to IPv6 sub block corruption. An attacker could exploit this vulnerability by polling the affected device IPv6 information. An exploit could allow the attacker to trigger high CPU usage or a reload of the device. Known Affected Releases: Denali-16.3.1. Cisco Bug IDs: CSCvb14640.	2017-09-07	not yet calculated	CVE-2017-12211 BID(link is external) SECTRAC K(link is external) CONFIRM (link is external) CONFIRM (link is external)
cisco -- ios_and_ios_xe	A vulnerability in the UDP processing code of Cisco IOS 15.1, 15.2, and 15.4 and IOS XE 3.14 through 3.18 could allow an unauthenticated, remote attacker to cause the input queue of an affected system to hold UDP packets, causing an interface queue wedge and a denial of service (DoS) condition. The vulnerability is due to Cisco IOS Software application changes that create UDP sockets and leave the sockets idle without closing them. An attacker could exploit this vulnerability by sending UDP packets with a destination port of 0 to an affected device. A successful	2017-09-07	not yet calculated	CVE-2017-6627 BID(link is external) SECTRAC K(link is external) CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploit could allow the attacker to cause UDP packets to be held in the input interfaces queue, resulting in a DoS condition. The input interface queue will stop holding UDP packets when it receives 250 packets. Cisco Bug IDs: CSCup10024, CSCva55744, CSCva95506.			
cisco -- ios_xe	A vulnerability in the USB-modem code of Cisco IOS XE Software running on Cisco ASR 920 Series Aggregation Services Routers could allow an authenticated, local attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to improper input validation of the platform usb modem command in the CLI of the affected software. An attacker could exploit this vulnerability by modifying the platform usb modem command in the CLI of an affected device. A successful exploit could allow the attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. Cisco Bug IDs: CSCve48949.	2017-09-07	not yet calculated	CVE-2017-6796 BID(link is external) SECTRACK(link is external) CONFIRM(link is external)
cisco -- ios_xe	A vulnerability in the dynamic access control list (ACL) feature of Cisco IOS XE Software running on Cisco Catalyst 4000 Series Switches could allow an unauthenticated, adjacent attacker to cause dynamic ACL assignment to fail and the port to fail open. This could allow the attacker to pass traffic to the default VLAN of the affected port. The vulnerability is due to an uncaught error condition that may occur during the reassignment of the auth-default-ACL dynamic ACL to a switch port	2017-09-07	not yet calculated	CVE-2017-12213 BID(link is external) SECTRACK(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	after 802.1x authentication fails. A successful exploit of this issue could allow a physically adjacent attacker to bypass 802.1x authentication and cause the affected port to fail open, allowing the attacker to pass traffic to the default VLAN of the affected switch port. Cisco Bug IDs: CSCvc72751.			
cisco -- ios_xe	A vulnerability in the USB-modem code of Cisco IOS XE Software running on Cisco ASR 920 Series Aggregation Services Routers could allow an authenticated, local attacker to overwrite arbitrary files on the underlying operating system of an affected device. The vulnerability is due to improper input validation of the platform usb modem command in the CLI of the affected software. An attacker could exploit this vulnerability by modifying the platform usb modem command in the CLI of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the underlying operating system of an affected device. Cisco Bug IDs: CSCvf10783.	2017-09-07	not yet calculated	CVE-2017-6795 BID(link is external) SECTRAC K(link is external) CONFIRM (link is external)
cisco -- iot_field_network_director	A vulnerability in the TCP throttling process for Cisco IoT Field Network Director (IoT-FND) could allow an unauthenticated, remote attacker to cause the system to consume additional memory, eventually forcing the device to restart, aka Memory Exhaustion. The vulnerability is due to insufficient rate-limiting protection. An attacker could exploit this vulnerability by sending a high rate of TCP packets to a specific group of open listening ports on a targeted device. An exploit could allow the attacker to cause the	2017-09-07	not yet calculated	CVE-2017-6780 BID(link is external) CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	system to consume additional memory. If enough available memory is consumed, the system will restart, creating a temporary denial of service (DoS) condition. The DoS condition will end after the device has finished the restart process. This vulnerability affects the following Cisco products: Connected Grid Network Management System, if running a software release prior to IoT-FND Release 4.0; IoT Field Network Director, if running a software release prior to IoT-FND Release 4.0. Cisco Bug IDs: CSCvc77164.			
cisco -- ir800_integrated_services_router_software	A vulnerability in the ROM Monitor (ROMMON) code of Cisco IR800 Integrated Services Router Software could allow an unauthenticated, local attacker to boot an unsigned Hypervisor on an affected device and compromise the integrity of the system. The vulnerability is due to insufficient sanitization of user input. An attacker who can access an affected router via the console could exploit this vulnerability by entering ROMMON mode and modifying ROMMON variables. A successful exploit could allow the attacker to execute arbitrary code and install a malicious version of Hypervisor firmware on an affected device. Cisco Bug IDs: CSCvb44027.	2017-09-07	not yet calculated	CVE-2017-12223 SECTRAC K(link is external) CONFIRM (link is external)
cisco -- meeting server	A vulnerability in the ability for guest users to join meetings via a hyperlink with Cisco Meeting Server could allow an authenticated, remote attacker to enter a meeting with a hyperlink URL, even though access should be denied. The vulnerability is due to the incorrect implementation of the configuration	2017-09-07	not yet calculated	CVE-2017-12224 BID(link is external) SECTRAC K(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	setting Guest access via hyperlinks, which should allow the administrative user to prevent guest users from using hyperlinks to connect to meetings. An attacker could exploit this vulnerability by using a crafted hyperlink to connect to a meeting. An exploit could allow the attacker to connect directly to the meeting with a hyperlink, even though access should be denied. The attacker would still require a valid hyperlink and encoded secret identifier to be connected. Cisco Bug IDs: CSCve20873.			(link is external)
cisco -- meeting_server	A vulnerability in the CLI command-parsing code of Cisco Meeting Server could allow an authenticated, local attacker to perform command injection and escalate their privileges to root. The attacker must first authenticate to the application with valid administrator credentials. The vulnerability is due to insufficient validation of user-supplied input at the CLI for certain commands. An attacker could exploit this vulnerability by authenticating to the affected application and submitting a crafted CLI command for execution at the Cisco Meeting Server CLI. An exploit could allow the attacker to perform command injection and escalate their privilege level to root. Vulnerable Products: This vulnerability exists in Cisco Meeting Server software versions prior to and including 2.0, 2.1, and 2.2. Cisco Bug IDs: CSCvf53830.	2017-09-07	not yet calculated	CVE-2017-6794 BID(link is external) SECTRAC K(link is external) CONFIRM (link is external)
cisco -- prime_collaboration_provisioning_tool	A vulnerability in the Inventory Management feature of Cisco Prime Collaboration Provisioning Tool could allow an authenticated, remote attacker to view sensitive	2017-09-07	not yet calculated	CVE-2017-6793 SECTRAC K(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	information on the system. The vulnerability is due to insufficient protection of restricted information. An attacker could exploit this vulnerability by accessing unauthorized information via the user interface. Cisco Bug IDs: CSCvd61932.			CONFIRM (link is external)
cisco -- prime_collaboration_provisioning_tool	A vulnerability in the batch provisioning feature in Cisco Prime Collaboration Provisioning Tool could allow an authenticated, remote attacker to overwrite system files as root. The vulnerability is due to lack of input validation of the parameters in BatchFileName and Directory. An attacker could exploit this vulnerability by manipulating the parameters of the batch action file function. Cisco Bug IDs: CSCvd61766.	2017-09-07	not yet calculated	CVE-2017-6792 BID(link is external) SECTRAC K(link is external) CONFIRM (link is external)
cisco -- prime_lan_management_solution	A vulnerability in the web functionality of the Cisco Prime LAN Management Solution could allow an authenticated, remote attacker to hijack another user's administrative session, aka a Session Fixation Vulnerability. The vulnerability is due to the reuse of a preauthentication session token as part of the postauthentication session. An attacker could exploit this vulnerability by obtaining the presession token ID. An exploit could allow an attacker to hijack an existing user's session. Known Affected Releases 4.2(5). Cisco Bug IDs: CSCvf58392.	2017-09-07	not yet calculated	CVE-2017-12225 SECTRAC K(link is external) CONFIRM (link is external) CONFIRM (link is external)
cisco -- socialminer	A vulnerability in the web-based user interface of Cisco SocialMiner could allow an unauthenticated, remote attacker to have read and write access to information stored in the affected system. The vulnerability is	2017-09-07	not yet calculated	CVE-2017-12216 BID(link is external) SECTRAC K(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	due to improper handling of XML External Entity (XXE) entries when parsing an XML file. An attacker could exploit this vulnerability by convincing the administrator of an affected system to import a crafted XML file with malicious entries, which could allow the attacker to read and write files and execute remote code within the application. Cisco Bug IDs: CSCvf47946.			external) CONFIRM (link is external)
cisco -- unified_intelligence_center	A vulnerability in the Trust Verification Service (TVS) of Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper handling of Transport Layer Security (TLS) traffic by the affected software. An attacker could exploit this vulnerability by generating incomplete traffic streams. A successful exploit could allow the attacker to deny access to the TVS for an affected device, resulting in a DoS condition, until an administrator restarts the service. Known Affected Releases 10.0(1.10000.24) 10.5(2.10000.5) 11.0(1.10000.10) 9.1(2.10000.28). Cisco Bug IDs: CSCux21905.	2017-09-07	not yet calculated	CVE-2017-6791 BID(link is external) SECTRAC K(link is external) CONFIRM (link is external) CONFIRM (link is external)
cisco -- unified_intelligence_center	A vulnerability in the Cisco Unified Intelligence Center web interface could allow an unauthenticated, remote attacker to impact the integrity of the system by executing a Document Object Model (DOM)-based, environment or client-side cross-site scripting (XSS) attack. The vulnerability occurs because user-supplied data in the DOM input is not validated. An attacker could	2017-09-07	not yet calculated	CVE-2017-6789 BID(link is external) SECTRAC K(link is external) CONFIRM (link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploit this vulnerability by sending crafted URLs that contain malicious DOM statements to the affected system. A successful exploit could allow the attacker to affect the integrity of the system by manipulating the database. Known Affected Releases 11.0(1)ES10. Cisco Bug IDs: CSCvf18325.			(link is external)
cisco -- unity_connection	A vulnerability in the web framework of Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web interface of an affected system. The vulnerability is due to insufficient input validation of certain parameters that are passed to the affected software via the HTTP GET and HTTP POST methods. An attacker who can convince a user to follow an attacker-supplied link could execute arbitrary script or HTML code in the user's browser in the context of an affected site. Known Affected Releases 10.5(2). Cisco Bug IDs: CSCvf25345.	2017-09-07	not yet calculated	CVE-2017-12212 BID(link is external) SECTRACK(link is external) CONFIRM (link is external) CONFIRM (link is external)
cisco -- yes_set-top_boxes	A vulnerability in the HTTP remote procedure call (RPC) service of set-top box (STB) receivers manufactured by Cisco for Yes could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability exists because the firmware of an affected device fails to handle certain XML values that are passed to the HTTP RPC service listening on the local subnet of the device. An attacker could exploit this vulnerability by submitting a malformed request to an affected device. A successful attack	2017-09-07	not yet calculated	CVE-2017-6631 BID(link is external) CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could cause the affected device to restart, resulting in a DoS condition. Yes has updated the affected devices with firmware that addresses this vulnerability. Customers are not required to take action. Vulnerable Products: This vulnerability affects YesMaxTotal, YesMax HD, and YesQuattro STB devices. Cisco Bug IDs: CSCvd08812.			
concrete5 -- concrete5	SQL injection vulnerability in Concrete5 5.7.3.1.	2017-09-07	not yet calculated	CVE-2015-4724 MISC(link is external)
concrete5 -- concrete5	Multiple cross-site scripting (XSS) vulnerabilities in Concrete5 5.7.3.1.	2017-09-07	not yet calculated	CVE-2015-4721 MISC(link is external)
d-link -- dir-600l	Session fixation vulnerability in D-Link DIR-600L routers (rev. Ax) with firmware before FW1.17.B01 allows remote attackers to hijack web sessions via unspecified vectors.	2017-09-07	not yet calculated	CVE-2016-10405 CONFIRM
dayrui -- finecms	The checktitle function in controllers/member/api.php in dayrui FineCms 5.0.11 has XSS related to the module field.	2017-09-07	not yet calculated	CVE-2017-14192 MISC(link is external)
dayrui -- finecms	The out function in controllers/member/Login.php in dayrui FineCms 5.0.11 has XSS related to the Referer HTTP header with Internet Explorer.	2017-09-07	not yet calculated	CVE-2017-14194 MISC(link is external)
dayrui -- finecms	The oauth function in controllers/member/api.php in dayrui FineCms 5.0.11 has XSS related to the Referer HTTP header with Internet Explorer.	2017-09-07	not yet calculated	CVE-2017-14193 MISC(link is external)
dayrui -- finecms	The call_msg function in controllers/Form.php in dayrui FineCms 5.0.11 might have XSS related to the Referer HTTP header with Internet Explorer.	2017-09-07	not yet calculated	CVE-2017-14195 MISC(link is external)
devscripts -- devscripts	Argument injection vulnerability in devscripts before 2.15.7 allows	2017-09-06	not yet	CVE-2015-5705

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote attackers to write to arbitrary files via a crafted symlink and crafted filename.		calculated	FEDORA FEDORA MLIST(link is external) CONFIRM CONFIRM CONFIRM (link is external)
diving_log -- diving_log	XXE in Diving Log 6.0 allows attackers to remotely view local files through a crafted dive.xml file that is mishandled during a Subsurface import.	2017-09-08	not yet calculated	CVE-2017-9095 MISC(link is external)
django -- django	In Django 1.10.x before 1.10.8 and 1.11.x before 1.11.5, HTML autoescaping was disabled in a portion of the template for the technical 500 debug page. Given the right circumstances, this allowed a cross-site scripting attack. This vulnerability shouldn't affect most production sites since you shouldn't run with "DEBUG = True" (which makes this page accessible) in your production settings.	2017-09-07	not yet calculated	CVE-2017-12794 BID(link is external) SECTRACK(link is external) CONFIRM (link is external)
epicor_crs -- retail_store	The help window in Epicor CRS Retail Store before 3.2.03.01.008 allows local users to execute arbitrary code by injecting Javascript into the window source to create a button that spawns a command shell.	2017-09-06	not yet calculated	CVE-2015-2210 MISC(link is external) BUGTRAQ(link is external)
etherpad -- etherpad	Directory traversal vulnerability in node/hooks/express/tests.js in Etherpad frontend tests before 1.6.1.	2017-09-07	not yet calculated	CVE-2015-4085 MLIST(link is external) CONFIRM (link is external)
ffmpeg -- ffmpeg	In libavformat/asfdec_f.c in FFmpeg 3.3.3, a DoS in	2017-09-08	not yet	CVE-2017-14223

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	asf_build_simple_index() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted ASF file, which claims a large "ict" field in the header but does not contain sufficient backing data, is provided, the for loop would consume huge CPU and memory resources, since there is no EOF check inside the loop.		calculated	CONFIRM (link is external)
ffmpeg -- ffmpeg	The av_color_primaries_name function in libavutil/pixdesc.c in FFmpeg 3.3.3 may return a NULL pointer depending on a value contained in a file, but callers do not anticipate this, as demonstrated by the avcodec_string function in libavcodec/utils.c, leading to a NULL pointer dereference. (It is also conceivable that there is security relevance for a NULL pointer dereference in av_color_primaries_name calls within the ffprobe command-line program.)	2017-09-09	not yet calculated	CVE-2017-14225 MISC(link is external) MISC
ffmpeg -- ffmpeg	In libavformat/mov.c in FFmpeg 3.3.3, a DoS in read_tfra() due to lack of an EOF (End of File) check might cause huge CPU and memory consumption. When a crafted MOV file, which claims a large "item_count" field in the header but does not contain sufficient backing data, is provided, the loop would consume huge CPU and memory resources, since there is no EOF check inside the loop.	2017-09-08	not yet calculated	CVE-2017-14222 CONFIRM (link is external)
fiberhome -- user_end_routers_an1020-25	An issue was discovered on FiberHome User End Routers bearing model number AN1020-25 which could allow an attacker to easily restore a router to its factory settings by simply browsing to the link http://[Default-Router-	2017-09-07	not yet calculated	CVE-2017-14147 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	IP]/restoreinfo.cgi & execute it. Due to improper authentication on this page, the software accepts the request hence allowing attacker to reset the router to its default configurations which later could allow attacker to login to router by using default username/password.			
glibc -- glibc	The DNS stub resolver in the GNU C Library (glibc) before version 2.26, when EDNS support is enabled, will solicit large UDP responses from name servers, potentially simplifying off-path DNS spoofing attackers due to IP fragmentation.	2017-09-07	not yet calculated	CVE-2017-12133 FEDORA CONFIRM CONFIRM
gongjin_electronics -- t&w_wifi_repeater_be126	T&W WIFI Repeater BE126 allows remote authenticated users to execute arbitrary code via shell metacharacters in the user parameter to cgi-bin/webupg.	2017-09-07	not yet calculated	CVE-2017-13713 MISC(link is external) EXPLOIT-DB(link is external)
google -- android	A remote code execution vulnerability in the Android media framework (libhevc). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-36492741.	2017-09-08	not yet calculated	CVE-2017-0758 BID(link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in the Android libraries (libgdx). Product: Android. Versions: 7.1.1, 7.1.2, 8.0. Android ID: A-62218744.	2017-09-08	not yet calculated	CVE-2017-0753 BID(link is external) CONFIRM (link is external)
google -- android	A denial of service vulnerability in the Android media framework (libhevc). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-37615911.	2017-09-08	not yet calculated	CVE-2017-0773 BID(link is external) CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	A elevation of privilege vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-37662122.	2017-09-08	not yet calculated	CVE-2017-0769 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37351060. References: B-V2017060101.	2017-09-08	not yet calculated	CVE-2017-0786 BID(link is external) CONFIRM (link is external)
google -- android	A denial of service vulnerability in the Android media framework (libskia). Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID: A-37624243.	2017-09-08	not yet calculated	CVE-2017-0771 BID(link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in the Android media framework (libavc). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-36006815.	2017-09-08	not yet calculated	CVE-2017-0757 BID(link is external) CONFIRM (link is external)
google -- android	A information disclosure vulnerability in the Android media framework (audioflinger). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-38340117.	2017-09-08	not yet calculated	CVE-2017-0779 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37722328. References: B-V2017053103.	2017-09-08	not yet calculated	CVE-2017-0788 BID(link is external) CONFIRM (link is external)
google -- android	A information disclosure vulnerability in the Android media	2017-09-08	not yet	CVE-2017-0777

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	framework (n/a). Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID: A-38342499.		calculated	BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the MediaTek accessory detector driver. Product: Android. Versions: Android kernel. Android ID: A-36136137. References: M-ALPS03361477.	2017-09-08	not yet calculated	CVE-2017-0803 BID(link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in the Android media framework (libavc). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-38448381.	2017-09-08	not yet calculated	CVE-2017-0761 BID(link is external) CONFIRM (link is external)
google -- android	A information disclosure vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37305578. References: B-V2017052301.	2017-09-08	not yet calculated	CVE-2017-0792 BID(link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-36715268.	2017-09-08	not yet calculated	CVE-2017-0759 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the MediaTek accessory detector driver. Product: Android. Versions: Android kernel. Android ID: A-36198473. References: M-ALPS03361480.	2017-09-08	not yet calculated	CVE-2017-0795 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the MediaTek accessory detector driver. Product: Android. Versions: Android kernel. Android ID: A-	2017-09-08	not yet calculated	CVE-2017-0797 BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	62459766. References: M-ALPS03353854.			CONFIRM (link is external)
google -- android	A denial of service vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-62673844.	2017-09-08	not yet calculated	CVE-2017-0774 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the MediaTek kernel. Product: Android. Versions: Android kernel. Android ID: A-36100671. References: M-ALPS03365532.	2017-09-08	not yet calculated	CVE-2017-0798 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the MediaTek auxadc driver. Product: Android. Versions: Android kernel. Android ID: A-62458865. References: M-ALPS03353884, M-ALPS03353886, M-ALPS03353887.	2017-09-08	not yet calculated	CVE-2017-0796 BID(link is external) CONFIRM (link is external)
google -- android	A information disclosure vulnerability in the N/A memory subsystem. Product: Android. Versions: Android kernel. Android ID: A-35764946.	2017-09-08	not yet calculated	CVE-2017-0793 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the MediaTek lastbus. Product: Android. Versions: Android kernel. Android ID: A-36731602. References: M-ALPS03342072.	2017-09-08	not yet calculated	CVE-2017-0799 BID(link is external) CONFIRM (link is external)
google -- android	A denial of service vulnerability in the Android media framework (libavc). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-38115076.	2017-09-08	not yet calculated	CVE-2017-0772 BID(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				(link is external)
google -- android	A elevation of privilege vulnerability in the MediaTek kernel. Product: Android. Versions: Android kernel. Android ID: A-36232120. References: M-ALPS03384818.	2017-09-08	not yet calculated	CVE-2017-0802 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the Android media framework (libeffects). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62019992.	2017-09-08	not yet calculated	CVE-2017-0768 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the MediaTek teei. Product: Android. Versions: Android kernel. Android ID: A-37683975. References: M-ALPS03302988.	2017-09-08	not yet calculated	CVE-2017-0800 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37357704. References: B-V2017053101.	2017-09-08	not yet calculated	CVE-2017-0790 BID(link is external) CONFIRM (link is external)
google -- android	A information disclosure vulnerability in the Android media framework (n/a). Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID: A-62133227.	2017-09-08	not yet calculated	CVE-2017-0778 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the Android media framework (libmediaplayerservice). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-38234812.	2017-09-08	not yet calculated	CVE-2017-0770 BID(link is external) CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	A elevation of privilege vulnerability in the Upstream kernel scsi driver. Product: Android. Versions: Android kernel. Android ID: A-35644812.	2017-09-08	not yet calculated	CVE-2017-0794 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the MediaTek libmtkomxvdec. Product: Android. Versions: Android kernel. Android ID: A-38447970. References: M-ALPS03337980.	2017-09-08	not yet calculated	CVE-2017-0801 BID(link is external) CONFIRM (link is external)
google -- android	A information disclosure vulnerability in the Android media framework (n/a). Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-38496660.	2017-09-08	not yet calculated	CVE-2017-0776 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37685267. References: B-V2017053102.	2017-09-08	not yet calculated	CVE-2017-0789 BID(link is external) CONFIRM (link is external)
google -- android	A denial of service vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62673179.	2017-09-08	not yet calculated	CVE-2017-0775 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the Android media framework (libeffects). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37536407.	2017-09-08	not yet calculated	CVE-2017-0767 BID(link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in the Android media	2017-09-08	not yet	CVE-2017-0764

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	framework (libvorbis). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62872015.		calculated	BID(link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in the Android media framework (libhevc). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-62214264.	2017-09-08	not yet calculated	CVE-2017-0762 BID(link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in the Android media framework (libjhead). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37776688.	2017-09-08	not yet calculated	CVE-2017-0766 BID(link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in the Android media framework (libhevc). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62534693.	2017-09-08	not yet calculated	CVE-2017-0763 BID(link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62872863.	2017-09-08	not yet calculated	CVE-2017-0765 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37306719. References: B-V2017052302.	2017-09-08	not yet calculated	CVE-2017-0791 BID(link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 6.0, 6.0.1, 7.0,	2017-09-08	not yet calculated	CVE-2017-0760 BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	7.1.1, 7.1.2. Android ID: A-37237396.			CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the Android system (nfc). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37287958.	2017-09-08	not yet calculated	CVE-2017-0784 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the Android framework (windowmanager). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-62196835.	2017-09-08	not yet calculated	CVE-2017-0752 BID(link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-34621073.	2017-09-08	not yet calculated	CVE-2017-0756 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the Android libraries (libminikin). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-32178311.	2017-09-08	not yet calculated	CVE-2017-0755 BID(link is external) CONFIRM (link is external)
google -- android	A denial of service vulnerability in the Android runtime (android messenger). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-37742976.	2017-09-08	not yet calculated	CVE-2017-0780 BID(link is external) CONFIRM (link is external)
google -- android	A elevation of privilege vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37722970. References: B-V2017053104.	2017-09-08	not yet calculated	CVE-2017-0787 BID(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				(link is external)
graphicsmagick -- graphicsmagick	The ReadSUNImage function in coders/sun.c in GraphicsMagick 1.3.26 has an issue where memory allocation is excessive because it depends only on a length field in a header. This may lead to remote denial of service in the MagickMalloc function in magick/memory.c.	2017-09-06	not yet calculated	CVE-2017-14165 MISC(link is external) MISC
huawei -- e5756s	Huawei E5756S before V200R002B146D23SP00C00 allows remote attackers to read device configuration information, enable PIN/PUK authentication, and perform other unspecified actions.	2017-09-07	not yet calculated	CVE-2015-4629 BID(link is external) CONFIRM (link is external)
ibm -- content_navigator_&_cmis	IBM Content Navigator & CMIS 2.0.3, 3.0.0, and 3.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 129577.	2017-09-07	not yet calculated	CVE-2017-1502 CONFIRM (link is external) MISC(link is external)
ibm -- emptoris_supplier_lifecycle_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: 120658.	2017-09-07	not yet calculated	CVE-2017-1098 CONFIRM (link is external) MISC(link is external)
ibm -- flex_system	Cross-site request forgery (CSRF) vulnerability in IBM Flex System EN6131 40Gb Ethernet and IB6131 40Gb Infiniband Switch firmware 3.4.0000 and earlier.	2017-09-07	not yet calculated	CVE-2014-9565 BID(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				(link is external)
ibm -- websphere_portal_web_content_manager	IBM WebSphere Portal and Web Content Manager 6.1, 7.0, and 8.0 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: 123558.	2017-09-07	not yet calculated	CVE-2017-1189 CONFIRM (link is external) SECTRAC K(link is external) MISC(link is external)
idapauth-fork -- idapauth-fork	Idapauth-fork before 2.3.3 allows remote attackers to perform LDAP injection attacks via a crafted username.	2017-09-06	not yet calculated	CVE-2015-7294 MLIST(link is external) MLIST(link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	A heap-based buffer overflow in WritePCXImage in coders/pcx.c in ImageMagick 7.0.6-8 Q16 allows remote attackers to cause a denial of service or code execution via a crafted file.	2017-09-08	not yet calculated	CVE-2017-14224 CONFIRM (link is external)
intel -- firmware_for_multiple_products	Intel Active Management Technology, Intel Standard Manageability, and Intel Small Business Technology firmware versions 11.0.25.3001 and 11.0.26.3000 can be upgraded to firmware version 11.6.x.1xxx which is vulnerable to CVE-2017-5689 and can be performed by a local user with administrative privileges.	2017-09-05	not yet calculated	CVE-2017-5698 CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
intelbras -- wireless_n_router_firmware	XSS (persistent) on the Intelbras Wireless N 150Mbps router with firmware WRN 240 allows attackers to steal wireless credentials without being connected to the network, related to userRpm/popupSiteSurveyRpm.htm and userRpm/WlanSecurityRpm.htm. The attack vector is a crafted ESSID, as demonstrated by an "airbase-ng -e" command.	2017-09-07	not yet calculated	CVE-2017-14219 MISC(link is external) EXPLOIT-DB(link is external)
jasper -- jasper	There is an infinite loop in the jpc_dec_tileinit function in jpc/jpc_dec.c of JasPer 2.0.13. It will lead to a remote denial of service attack.	2017-09-09	not yet calculated	CVE-2017-14229 MISC(link is external)
joomla! -- joomla!	The Googlemaps plugin before 3.1 for Joomla! allows remote attackers to cause a denial of service via the url parameter to plugin_googlemap2_proxy.php.	2017-09-07	not yet calculated	CVE-2013-7428 FULLDISC CONFIRM (link is external) MLIST(link is external) MLIST(link is external)
joomla! -- joomla!	Vulnerability in Easy Joomla Backup v3.2.4. The software creates a copy of the backup in the web root with an easily guessable filename.	2017-09-08	not yet calculated	CVE-2017-2550 MISC(link is external)
kamailio -- kamailio	The kamcmd administrative utility and default configuration in kamailio before 4.3.0 use /tmp/kamailio_ctl.	2017-09-07	not yet calculated	CVE-2015-1590 MLIST(link is external) CONFIRM CONFIRM (link is external) CONFIRM (link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				external) CONFIRM (link is external)
lexmark -- scan_to_network	Lexmark Scan To Network (SNF) 3.2.9 and earlier stores network configuration credentials in plaintext and transmits them in requests, which allows remote attackers to obtain sensitive information via requests to (1) cgi-bin/direct/printer/prtappauth/apps/snfDestServlet or (2) cgi-bin/direct/printer/prtappauth/apps/ImportExportServlet.	2017-09-07	not yet calculated	CVE-2017-13771 MISC(link is external) FULLDISC
libgd2 -- libgd2	Double free vulnerability in the gdImagePngPtr function in libgd2 before 2.2.5 allows remote attackers to cause a denial of service via vectors related to a palette with no colors.	2017-09-07	not yet calculated	CVE-2017-6362 DEBIAN CONFIRM (link is external) CONFIRM (link is external) FEDORA
libwpd -- libwpd	WP1StylesListener.cpp, WP5StylesListener.cpp, and WP42StylesListener.cpp in libwpd 0.10.1 mishandle iterators, which allows remote attackers to cause a denial of service (heap-based buffer over-read in the WPXTableList class in WPXTable.cpp). This vulnerability can be triggered in LibreOffice before 5.3.7. It may lead to suffering a remote attack against a LibreOffice application.	2017-09-09	not yet calculated	CVE-2017-14226 MISC MISC(link is external) MISC MISC(link is external) MISC(link is external) MISC(link is external)
lightdm -- lightdm	Array index error in LightDM (aka Light Display Manager) 1.14.3, 1.16.x before 1.16.6 when the XDMCP server is enabled allows remote attackers to cause a denial of service (process crash) via an	2017-09-06	not yet calculated	CVE-2015-8316 MLIST(link is external) CONFIRM (link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	XDMCP request packet with no address.			external) CONFIRM (link is external)
linux -- linux_kernel	The driver_override implementation in drivers/base/platform.c in the Linux kernel before 4.12.1 allows local users to gain privileges by leveraging a race condition between a read operation and a store operation that involve different overrides.	2017-09-08	not yet calculated	CVE-2017-12146 CONFIRM CONFIRM CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	The mkdumprd script called "dracut" in the current working directory "." allows local users to trick the administrator into executing code as root.	2017-09-08	not yet calculated	CVE-2016-5759 SUSE MLIST(link is external)
linux -- linux_kernel	Audit before 2.4.4 in Linux does not sanitize escape characters in filenames.	2017-09-06	not yet calculated	CVE-2015-5186 MLIST(link is external) BID(link is external) CONFIRM (link is external) CONFIRM (link is external)
mediatek -- mediatek	A elevation of privilege vulnerability in the MediaTek mmc driver. Product: Android. Versions: Android kernel. Android ID: A-36274676. References: M-ALPS03361487.	2017-09-08	not yet calculated	CVE-2017-0804 BID(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				(link is external)
mongodb -- libbson	In MongoDB libbson 1.7.0, the bson_iter_codewscope function in bson-iter.c miscalculates a bson_utf8_validate length argument, which allows remote attackers to cause a denial of service (heap-based buffer over-read in the bson_utf8_validate function in bson-utf8.c), as demonstrated by bson-to-json.c.	2017-09-09	not yet calculated	CVE-2017-14227 MISC(link is external) MISC(link is external) MISC(link is external)
mongoose_web_server -- mongoose_web_server	Cross-site request forgery (CSRF) vulnerability in Mongoose Web Server before 6.9 allows remote attackers to hijack the authentication of users for requests that modify Mongoose.conf via a request to __mg_admin?save. NOTE: this issue can be leveraged to execute arbitrary code remotely.	2017-09-07	not yet calculated	CVE-2017-11567 MISC FULLDISC EXPLOIT-DB(link is external)
mp3gain -- mp3gain	The "mpglibDBL/layer3.c" file in MP3Gain 1.5.2.r2 has a vulnerability which results in a read access violation when opening a crafted MP3 file.	2017-09-07	not yet calculated	CVE-2017-12912 MISC(link is external)
mp3gain -- mp3gain	The "apetag.c" file in MP3Gain 1.5.2.r2 has a vulnerability which results in a stack memory corruption when opening a crafted MP3 file.	2017-09-07	not yet calculated	CVE-2017-12911 MISC(link is external)
mp4tools -- aacplusenc	DeleteBitBuffer in libbitbuf/bitbuffer.c in mp4tools aacplusenc 0.17.5 allows remote attackers to cause a denial of service (invalid memory write, SEGV on unknown address 0x000000000030, and application crash) or possibly have unspecified other impact via a crafted .wav file, aka a NULL pointer dereference.	2017-09-07	not yet calculated	CVE-2017-14181 MISC MISC(link is external)
nasm -- nasm	In Netwide Assembler (NASM) 2.14rc0, there is an illegal address access in the function paste_tokens() in preproc.c, aka a NULL pointer	2017-09-09	not yet calculated	CVE-2017-14228 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	dereference. It will lead to remote denial of service.			
national_instruments -- labview	An exploitable memory corruption vulnerability exists in the RSRC segment parsing functionality of LabVIEW 2017, LabVIEW 2016, LabVIEW 2015, and LabVIEW 2014. A specially crafted Virtual Instrument (VI) file can cause an attacker controlled looping condition resulting in an arbitrary null write. An attacker controlled VI file can be used to trigger this vulnerability and can potentially result in code execution.	2017-09-05	not yet calculated	CVE-2017-2779 CONFIRM (link is external) BID(link is external) MISC(link is external) MISC(link is external)
nexsusphp -- nexsusphp	Cross-site request forgery (CSRF) vulnerability in NexusPHP 1.5 allows remote attackers to hijack the authentication of users for requests that (1) send manas via a request to mybonus.php or (2) add administrators via unspecified vectors.	2017-09-07	not yet calculated	CVE-2017-12838 MISC(link is external)
nexsusphp -- nexsusphp	Multiple cross-site scripting (XSS) vulnerabilities in NexusPHP allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to (1) cheaters.php or (2) confirm_resend.php.	2017-09-07	not yet calculated	CVE-2017-12906 MISC(link is external) MISC(link is external)
ocaml -- ocaml	OCaml compiler allows attackers to have unspecified impact via unknown vectors, a similar issue to CVE-2017-9772 "but with much less impact."	2017-09-07	not yet calculated	CVE-2017-9779 CONFIRM (link is external) MLIST(link is external)
opendreambox -- opendreambox	enigma2-plugins/blob/master/webadmin/src/WebChilds/Script.py in the webadmin plugin for opendreambox 2.0.0 allows remote attackers to execute arbitrary OS commands via shell	2017-09-04	not yet calculated	CVE-2017-14135 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	metacharacters in the command parameter to the /script URI.			
openjpeg -- openjpeg	A size-validation issue was discovered in opj_j2k_write_sot in lib/openjp2/j2k.c in OpenJPEG 2.2.0. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service (heap-based buffer overflow affecting opj_write_bytes_LE in lib/openjp2/cio.c) or possibly remote code execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-14152.	2017-09-06	not yet calculated	CVE-2017-14164 MISC MISC(link is external) MISC(link is external)
openldap -- openldap	slapd in OpenLDAP 2.4.45 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill `cat /pathname`" command, as demonstrated by openldap-initscript.	2017-09-05	not yet calculated	CVE-2017-14159 MISC
opw_fuel_management_systems -- sitesentinel_integra_consoles	A Missing Authentication for Critical Function issue was discovered in OPW Fuel Management Systems SiteSentinel Integra 100, SiteSentinel Integra 500, and SiteSentinel iSite ATG consoles with the following software versions: older than V175, V175-V189, V191-V195, and V16Q3.1. An attacker may create an application user account to gain administrative privileges.	2017-09-08	not yet calculated	CVE-2017-12733 BID(link is external) MISC
opw_fuel_management_systems -- sitesentinel_integra_consoles	A SQL Injection issue was discovered in OPW Fuel Management Systems SiteSentinel Integra 100, SiteSentinel Integra 500, and SiteSentinel iSite ATG consoles with the following software versions: older than V175, V175-V189, V191-V195, and V16Q3.1. The application is vulnerable to injection of	2017-09-08	not yet calculated	CVE-2017-12731 BID(link is external) MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	malicious SQL queries via the input from the client.			
ossec -- ossec	syscheck/seechanges.c in OSSEC 2.7 through 2.8.1 on NIX systems allows local users to execute arbitrary code as root.	2017-09-07	not yet calculated	CVE-2015-3222 MISC(link is external) MLIST(link is external) BID(link is external) CONFIRM (link is external)
palo_alto -- pan-os	Cross-site scripting (XSS) vulnerability in the GlobalProtect internal and external gateway interface in Palo Alto Networks PAN-OS before 6.1.18, 7.0.x before 7.0.17, 7.1.x before 7.1.12, and 8.0.x before 8.0.3 allows remote attackers to inject arbitrary web script or HTML via vectors related to improper request parameter validation.	2017-09-07	not yet calculated	CVE-2017-12416 CONFIRM (link is external) BID(link is external) SECTRAC K(link is external)
palo_alto -- pan_os	XML external entity (XXE) vulnerability in the GlobalProtect internal and external gateway interface in Palo Alto Networks PAN-OS before 6.1.18, 7.0.x before 7.0.17, 7.1.x before 7.1.12, and 8.0.x before 8.0.3 allows remote attackers to obtain sensitive information, cause a denial of service, or conduct server-side request forgery (SSRF) attacks via unspecified vectors.	2017-09-07	not yet calculated	CVE-2017-9458 CONFIRM (link is external) BID(link is external) SECTRAC K(link is external)
pivotal -- cloud_foundry	The identity zones feature in Pivotal Cloud Foundry 208 through 229; UAA 2.0.0 through 2.7.3 and 3.0.0; UAA-Release 2 through 4, when configured with multiple identity zones; and Elastic Runtime 1.6.0 through 1.6.13 allows remote authenticated users with privileges in	2017-09-07	not yet calculated	CVE-2016-0732 CONFIRM (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	one zone to gain privileges and perform operations on a different zone via unspecified vectors.			
pivotal -- cloud_foundry	In Single Sign-On for Pivotal Cloud Foundry (PCF) 1.3.x versions prior to 1.3.4 and 1.4.x versions prior to 1.4.3, an XXE (XML External Entity) attack was discovered in the Single Sign-On service dashboard. Privileged users can in some cases upload malformed XML leading to exposure of data on the Single Sign-On service broker file system.	2017-09-08	not yet calculated	CVE-2017-8040 BID(link is external) CONFIRM (link is external)
pivotal -- cloud_foundry	In Single Sign-On for Pivotal Cloud Foundry (PCF) 1.3.x versions prior to 1.3.4 and 1.4.x versions prior to 1.4.3, a user can execute a XSS attack on certain Single Sign-On service UI pages by inputting code in the text field for an organization name.	2017-09-08	not yet calculated	CVE-2017-8041 BID(link is external) CONFIRM (link is external)
pragyan -- pragyan	SQL injection vulnerability in Pragyan CMS 3.0.	2017-09-07	not yet calculated	CVE-2015-4627 MISC(link is external)
qemu -- qemu	Integer overflow in the load_multiboot function in hw/i386/multiboot.c in QEMU (aka Quick Emulator) allows local guest OS users to execute arbitrary code on the host via crafted multiboot header address values, which trigger an out-of-bounds write.	2017-09-08	not yet calculated	CVE-2017-14167 MLIST(link is external) MLIST
qtwebkit -- qt5	qt5-qtwebkit before 5.4 records private browsing URLs to its favicon database, WebpageIcons.db.	2017-09-07	not yet calculated	CVE-2015-8079 MLIST(link is external) CONFIRM (link is external) CONFIRM
ruby -- ruby	The URI.decode_www_form_component	2017-09-06	not yet	CVE-2014-6438

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	method in Ruby before 1.9.2-p330 allows remote attackers to cause a denial of service (catastrophic regular expression backtracking, resource consumption, or application crash) via a crafted string.		calculated	MLIST(link is external) SECTRACK(link is external) CONFIRM CONFIRM
safrengo -- safrengo	SQL injection vulnerability in Sefrengo before 1.6.5 beta2.	2017-09-07	not yet calculated	CVE-2015-5052 CONFIRM
simple-php-captcha -- simple-php-captcha	simple-php-captcha before commit 9d65a945029c7be7bb6bc893759e74c5636be694 allows remote attackers to automatically generate the captcha response by running the same code on the client-side.	2017-09-06	not yet calculated	CVE-2015-6250 MLIST(link is external) CONFIRM(link is external) CONFIRM(link is external)
soreco -- xpert_line	Soreco Xpert.Line 3.0 allows local users to spoof users and consequently gain privileges by intercepting a Windows API call.	2017-09-07	not yet calculated	CVE-2015-3442 MISC(link is external) FULLDISC BUGTRAQ(link is external) BID(link is external) MISC(link is external)
spina -- spina	Cross-site request forgery (CSRF) vulnerability in Spina before commit bfe44f289e336f80b6593032679300c493735e75.	2017-09-07	not yet calculated	CVE-2015-4619 MLIST(link is external) BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC(link is external)
strongswan -- strongswan	strongSwan 5.2.2 and 5.3.0 allows remote attackers to cause a denial of service (daemon crash) or execute arbitrary code.	2017-09-07	not yet calculated	CVE-2015-3991 FEDORA FEDORA BID(link is external) CONFIRM (link is external) CONFIRM
svn-workbench -- svn-workbench	svn-workbench 1.6.2 and earlier on a system with xeyes installed allows local users to execute arbitrary commands by using the "Command Shell" menu item while in the directory trunk/$(xeyes).	2017-09-06	not yet calculated	CVE-2015-0853 MISC MLIST(link is external) MISC MISC(link is external) CONFIRM (link is external)
symantec -- proxyclient	Symantec ProxyClient 3.4 for Windows is susceptible to a privilege escalation vulnerability. A malicious local Windows user can, under certain circumstances, exploit this vulnerability to escalate their privileges on the system and execute arbitrary code with LocalSystem privileges.	2017-09-01	not yet calculated	CVE-2017-13674 BID(link is external) CONFIRM (link is external)
synology -- photo_station	Server-side request forgery (SSRF) vulnerability in file_upload.php in Synology Photo Station before 6.7.4-3433 and 6.3-2968 allows remote authenticated users to download arbitrary local files via the url parameter.	2017-09-08	not yet calculated	CVE-2017-12071 CONFIRM (link is external)
synology -- photo_station	Directory traversal vulnerability in synphotoio in Synology Photo Station before 6.7.4-3433 and 6.3-2968 allows remote authenticated	2017-09-08	not yet calculated	CVE-2017-11162 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	users to read arbitrary files via unspecified vectors.			(link is external)
synology -- photo_station	Multiple SQL injection vulnerabilities in Synology Photo Station before 6.7.4-3433 and 6.3-2968 allow remote attackers to execute arbitrary SQL commands via the (1) article_id parameter to label.php; or (2) type parameter to synotheme.php.	2017-09-08	not yet calculated	CVE-2017-11161 CONFIRM (link is external)
tinfoil -- devise-two-factor	Tinfoil Devise-two-factor before 2.0.0 does not strictly follow section 5.2 of RFC 6238 and does not "burn" a successfully validated one-time password (aka OTP), which allows remote or physically proximate attackers with a target user's login credentials to log in as said user by obtaining the OTP through performing a man-in-the-middle attack between the provider and verifier, or shoulder surfing, and replaying the OTP in the current time-step.	2017-09-06	not yet calculated	CVE-2015-7225 MLIST(link is external) MLIST(link is external) BID(link is external) MISC CONFIRM (link is external) CONFIRM (link is external)
wibu_systems -- codemeter	Cross-site scripting (XSS) vulnerability in the "advanced settings - time server" module in Wibu-Systems CodeMeter before 6.50b allows remote attackers to inject arbitrary web script or HTML via the "server name" field in actions/ChangeConfiguration.html.	2017-09-07	not yet calculated	CVE-2017-13754 FULLDISC BUGTRAQ(link is external) EXPLOIT-DB(link is external) MISC(link is external)
wolf_cms -- wolf_cms	Wolf CMS 0.8.3.1 allows Cross-Site Scripting (XSS) attacks. The vulnerability exists due to insufficient sanitization of the file name in a "create-file-popup" action,	2017-09-08	not yet calculated	CVE-2017-11611 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and the directory name in a "create-directory-popup" action, in the HTTP POST method to the "/plugin/file_manager/" script (aka an /admin/plugin/file_manager/browse//URI).			
wordpress -- wordpress	SQL injection vulnerability in the WatuPRO plugin before 5.5.3.7 for WordPress allows remote attackers to execute arbitrary SQL commands via the watupro_questions parameter in a watupro_submit action to wp-admin/admin-ajax.php.	2017-09-07	not yet calculated	CVE-2017-9834 MISC(link is external) EXPLOIT-DB(link is external)
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Google Analyticator Wordpress Plugin before 6.4.9.3 rev @1183563.	2017-09-07	not yet calculated	CVE-2015-4697 MLIST MLIST(link is external) BID(link is external) MISC MISC
wordpress -- wordpress	SQL injection vulnerability in WordPress Tune Library plugin before 1.5.5.	2017-09-07	not yet calculated	CVE-2015-3314 MISC(link is external) MLIST(link is external) MLIST(link is external) BID(link is external) CONFIRM EXPLOIT-DB(link is external)
wordpress -- wordpress	SQL injection vulnerability in WordPress Community Events plugin before 1.4.	2017-09-07	not yet calculated	CVE-2015-3313 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MLIST(link is external) MLIST(link is external) BID(link is external) CONFIRM EXPLOIT-DB(link is external)
yast -- yast	The YaST2 network created files with world readable permissions which could have allowed local users to read sensitive material out of network configuration files, like passwords for wireless networks.	2017-09-08	not yet calculated	CVE-2011-3177 CONFIRM (link is external) CONFIRM (link is external)
zoho -- manageengine_firewall_analyzer	Zoho ManageEngine Firewall Analyzer 12200 has an unrestricted File Upload vulnerability in the "Group Chat" section. Any user can upload files with any extensions. By uploading a PHP file to the server, an attacker can cause it to execute in the server context, as demonstrated by /itplus/FileStorage/302/shell.jsp.	2017-09-04	not yet calculated	CVE-2017-14123 MISC(link is external) MISC(link is external)

Back to top