Vulnerability Summary for the Week of July 31, 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
cacti -- cacti	spikekill.php in Cacti before 1.1.16 might allow remote attackers to execute arbitrary code via the avgnan, outlier-start, or outlier-end parameter.	2017-08-01	7.5	CVE-2017-12065 BID(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST) devices allows remote attackers to execute arbitrary commands as root by leveraging local network access and connecting to the syseventd server, as demonstrated by copying configuration data into a readable filesystem.	2017-07-30	10.0	CVE-2017-9479 MISC(link is external)
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST) devices allows remote attackers to obtain root access to the Network Processor (NP) Linux system by enabling a TELNET daemon (through	2017-07-30	10.0	CVE-2017-9482 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVE-2017-9479 exploitation) and then establishing a TELNET session.			
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST) devices allows Network Processor (NP) Linux users to obtain root access to the Application Processor (AP) Linux system via shell metacharacters in commands.	2017-07-30	10.0	CVE-2017-9483 MISC(link is external)
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421733-160420a-CMCST); Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST); Cisco DPC3939B (firmware version dpc3939b-v303r204217-150321a-CMCST); Cisco DPC3941T (firmware version DPC3941_2.5s3_PROD_sey); and Arris TG1682G (eMTA&DOCSIS version 10.0.132.SIP.PC20.CT, software version TG1682_2.2p7s2_PROD_sey) devices allows remote attackers to execute arbitrary code via a specific (but unstated) exposed service. NOTE: the scope of this CVE does NOT include the concept of "Unnecessary Services" in general; the scope is only a single service that is unnecessarily exposed, leading to remote code execution. The	2017-07-30	7.5	CVE-2017-9521 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	details of that service might be disclosed at a later date.			
cisco -- mx011anm_firmware	The Comcast firmware on Motorola MX011ANM (firmware version MX011AN_2.9p6s1_PROD_sey) devices allows physically proximate attackers to execute arbitrary commands as root by pulling up the diagnostics menu on the set-top box, and then posting to a Web Inspector route.	2017-07-30	7.2	CVE-2017-9497 MISC(link is external)
etoilewebdesign -- ultimate_product_catalog	The Etoile Ultimate Product Catalog plugin 4.2.11 for WordPress has SQL injection with these wp-admin/admin-ajax.php POST actions: catalogue_update_order list-item, video_update_order video-item, image_update_order list-item, tag_group_update_order list_item, category_products_update_order category-product-item, custom_fields_update_order field-item, categories_update_order category-item, subcategories_update_order subcategory-item, and tags_update_order tag-list-item.	2017-08-02	7.5	CVE-2017-12199 MISC(link is external)
glpi-project -- glpi	SQL injection exists in front/devicesoundcard.php in GLPI before 9.1.5 via the start parameter.	2017-07-28	7.5	CVE-2017-11184 CONFIRM(link is external) CONFIRM(link is external)
ibm -- bigfix_platform	IBM Tivoli Endpoint Manager could allow a unauthorized user	2017-07-31	7.8	CVE-2017-1227

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to consume all resources and crash the system. IBM X-Force ID: 123906.			CONFIRM(link is external) MISC(link is external)
imagemagick -- imagemagick	The ReadDCMImage function in coders\dcm.c in ImageMagick 7.0.6-1 has an integer signedness error leading to excessive memory consumption via a crafted DCM file.	2017-08-02	7.1	CVE-2017-12140 BID(link is external) CONFIRM(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service.	2017-08-04	7.8	CVE-2017-12429 CONFIRM(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadMPCImage in coders/mpc.c, which allows attackers to cause a denial of service.	2017-08-04	7.8	CVE-2017-12430 CONFIRM(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadPCXImage in coders/pcx.c, which allows attackers to cause a denial of service.	2017-08-04	7.1	CVE-2017-12432 CONFIRM(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadSUNImage in coders/sun.c, which allows attackers to cause a denial of service.	2017-08-04	7.8	CVE-2017-12435 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
inversepath -- tenshi	Tenshi 0.15 creates a tenshi.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 tenshi.pid modification before a root script executes a "kill `cat /pathname/tenshi.pid`" command.	2017-07-30	7.8	CVE-2017-11746 MISC(link is external)
kiri -- tween	Untrusted search path vulnerability in Tween Ver1.6.6.0 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-08-02	9.3	CVE-2017-2279 JVN(link is external)
lame_project -- lame	There is a division-by-zero vulnerability in LAME 3.99.5, caused by a malformed input file.	2017-07-28	7.5	CVE-2017-11720 MISC(link is external)
microsoft -- outlook	Microsoft Outlook 2007 SP3, Outlook 2010 SP2, Outlook 2013 SP1, Outlook 2013 RT SP1, and Outlook 2016 as packaged in Microsoft Office allows a remote code execution vulnerability due to the way Microsoft Outlook parses specially crafted email messages, aka "Microsoft Office Outlook Memory Corruption Vulnerability"	2017-08-01	9.3	CVE-2017-8663 BID(link is external) SECTRACK(link is external) CONFIRM(link is external)
netcomm -- 4gt101w_bootloader	NetComm Wireless 4GT101W routers with Hardware: 0.01 / Software: V1.1.8.8 / Bootloader: 1.1.3 do not require authentication for logfile.html, status.html, or system_config.html.	2017-07-28	7.5	CVE-2017-11645 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nvidia -- gpu_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where the size of an input buffer is not validated which may lead to denial of service or potential escalation of privileges	2017-07-28	7.2	CVE-2017-6253 CONFIRM(link is external)
nvidia -- gpu_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where a pointer passed from an user to the driver is used without validation which may lead to denial of service or potential escalation of privileges.	2017-07-28	7.2	CVE-2017-6254 CONFIRM(link is external)
nvidia -- gpu_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where an improper input parameter handling may lead to a denial of service or potential escalation of privileges.	2017-07-28	7.2	CVE-2017-6255 CONFIRM(link is external)
openexif_project -- openexif	The ExifImageFile::readImage function in ExifImageFileRead.cpp in OpenExif 2.1.4 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted jpg file.	2017-07-31	7.1	CVE-2017-11118 MISC
timidity++_project -- timidity++	The play_midi function in playmidi.c in TiMidity++ 2.14.0 allows remote attackers to cause a denial of service (large loop	2017-07-31	7.1	CVE-2017-11549 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and CPU consumption) via a crafted mid file. NOTE: CPU consumption might be relevant when using the --background option.			
trendmicro -- control_manager	SQL Injection in Trend Micro Control Manager 6.0 causes Remote Code Execution when executing opcode 0x1b07 due to lack of proper user input validation in cmdHandlerTVCSCommander.dll. Fomerly ZDI-CAN-4560.	2017-08-02	7.5	CVE-2017-11383 BID(link is external) SECTRACK(link is external) MISC(link is external) MISC(link is external)
trendmicro -- control_manager	SQL Injection in Trend Micro Control Manager 6.0 causes Remote Code Execution when executing opcode 0x3b21 due to lack of proper user input validation in mdHandlerLicenseManager.dll. Fomerly ZDI-CAN-4561.	2017-08-02	7.5	CVE-2017-11384 BID(link is external) SECTRACK(link is external) MISC(link is external) MISC(link is external)
trendmicro -- control_manager	SQL Injection in Trend Micro Control Manager 6.0 causes Remote Code Execution when executing opcode 0x6b1b due to lack of proper user input validation in cmdHandlerStatusMonitor.dll. Formerly ZDI-CAN-4545.	2017-08-02	7.5	CVE-2017-11385 BID(link is external) SECTRACK(link is external) MISC(link is external) MISC(link is external)
trendmicro -- control_manager	SQL Injection in Trend Micro Control Manager 6.0 causes Remote Code Execution when executing opcode 0x4707 due to lack of proper user input	2017-08-02	7.5	CVE-2017-11386 BID(link is external) SECTRACK(li

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	validation in cmdHandlerNewReportScheduler.dll. Formerly ZDI-CAN-4549.			nk is external) MISC(link is external) MISC(link is external)
trendmicro -- control_manager	Directory traversal vulnerability in Trend Micro Control Manager 6.0 allows remote code execution by attackers able to drop arbitrary files in a web-facing directory. Formerly ZDI-CAN-4684.	2017-08-02	7.5	CVE-2017-11389 BID(link is external) SECTRACK(link is external) MISC(link is external) MISC(link is external)
trendmicro -- deep_discovery_director	A command injection vulnerability exists in Trend Micro Deep Discovery Director 1.1 that allows an attacker to restore accounts that can access the pre-configuration console.	2017-08-01	7.5	CVE-2017-11381 CONFIRM(link is external) MISC(link is external)
trendmicro -- interscan_messaging_security_virtual_appliance	Proxy command injection vulnerability in Trend Micro InterScan Messaging Virtual Appliance 9.0 and 9.1 allows remote attackers to execute arbitrary code on vulnerable installations. The specific flaw can be exploited by parsing the "t" parameter within modTMCSS Proxy. Formerly ZDI-CAN-4744.	2017-08-03	9.0	CVE-2017-11391 BID(link is external) MISC(link is external) MISC(link is external)
trendmicro -- officescan	Proxy command injection vulnerability in Trend Micro OfficeScan 11 and XG (12) allows remote attackers to execute arbitrary code on vulnerable installations. The specific flaw can be exploited by parsing the tr parameter	2017-08-03	10.0	CVE-2017-11393 BID(link is external) MISC(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	within Proxy.php. Formerly ZDI-CAN-4543.			

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arris -- tg1682g_firmware	The Comcast firmware on Cisco DPC3939B (firmware version dpc3939b-v303r204217-150321a-CMCST) devices allows configuration changes via CSRF.	2017-07-30	6.8	CVE-2017-9489 MISC(link is external)
artifex -- ghostscript	psi/ztoken.c in Artifex Ghostscript 9.21 mishandles references to the scanner state structure, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PostScript document, related to an out-of-bounds read in the igc_reloc_struct_ptr function in psi/igc.c.	2017-07-28	6.8	CVE-2017-11714 CONFIRM(link is external) CONFIRM(link is external)
bigtreecms -- bigtree_cms	SQL injection vulnerability in core\admin\auto-modules\forms\process.php in BigTree 4.2.18 allows remote authenticated users to execute arbitrary SQL commands via the tags array parameter.	2017-07-29	6.5	CVE-2017-11736 MISC(link is external)
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421733-160420a-CMCST) and DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST) devices sets the CM MAC address to a	2017-07-30	5.0	CVE-2017-9478 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	value with a two-byte offset from the MTA/VoIP MAC address, which indirectly allows remote attackers to discover hidden Home Security Wi-Fi networks by leveraging the embedding of the MTA/VoIP MAC address into the DNS hostname.			
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST) devices allows remote attackers to obtain unintended access to the Network Processor (NP) 169.254/16 IP network by adding a routing-table entry that specifies the LAN IP address as the router for that network.	2017-07-30	5.0	CVE-2017-9481 MISC(link is external)
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421733-160420a-CMCST) and DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST) devices allows remote attackers to discover a CM MAC address by sniffing Wi-Fi traffic and performing simple arithmetic calculations.	2017-07-30	5.0	CVE-2017-9484 MISC(link is external)
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST) devices allows remote attackers to write arbitrary data to a known /var/tmp/sess_* pathname by leveraging the device's operation in UI dev mode.	2017-07-30	5.0	CVE-2017-9485 MISC(link is external)
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST) devices allows remote	2017-07-30	5.0	CVE-2017-9486 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to compute password-of-the-day values via unspecified vectors.			
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST) and DPC3941T (firmware version DPC3941_2.5s3_PROD_sey) devices allows remote attackers to discover a WAN IPv6 IP address by leveraging knowledge of the CM MAC address.	2017-07-30	4.3	CVE-2017-9487 MISC(link is external)
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST) and DPC3941T (firmware version DPC3941_2.5s3_PROD_sey) devices allows remote attackers to access the web UI by establishing a session to the wan0 WAN IPv6 address and then entering unspecified hardcoded credentials. This wan0 interface cannot be accessed from the public Internet.	2017-07-30	5.8	CVE-2017-9488 MISC(link is external)
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421733-160420a-CMCST); Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST); Cisco DPC3939B (firmware version dpc3939b-v303r204217-150321a-CMCST); Cisco DPC3941T (firmware version DPC3941_2.5s3_PROD_sey); and Arris TG1682G (eMTA&DOCSIS version 10.0.132.SIP.PC20.CT, software version TG1682_2.2p7s2_PROD_sey) devices does not set the secure flag for cookies in an https session to an administration application, which	2017-07-30	5.0	CVE-2017-9491 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	makes it easier for remote attackers to capture these cookies by intercepting their transmission within an http session.			
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421733-160420a-CMCST); Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST); Cisco DPC3939B (firmware version dpc3939b-v303r204217-150321a-CMCST); Cisco DPC3941T (firmware version DPC3941_2.5s3_PROD_sey); and Arris TG1682G (eMTA&DOCSIS version 10.0.132.SIP.PC20.CT, software version TG1682_2.2p7s2_PROD_sey) devices does not include the HTTPOnly flag in a Set-Cookie header for administration applications, which makes it easier for remote attackers to obtain potentially sensitive information via script access to cookies.	2017-07-30	5.0	CVE-2017-9492 MISC(link is external)
cisco -- ios	Cisco IOS before 15.2(4)S6 does not initialize an unspecified variable, which might allow remote authenticated users to cause a denial of service (CPU consumption, watchdog timeout, crash) by walking specific SNMP objects.	2017-08-02	6.8	CVE-2012-5030 CISCO(link is external)
cisco -- mx011anm_firmware	The Comcast firmware on Motorola MX011ANM (firmware version MX011AN_2.9p6s1_PROD_sey) devices allows remote attackers to conduct successful forced-pairing attacks (between an RF4CE remote	2017-07-30	5.8	CVE-2017-9493 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and a set-top box) by repeatedly transmitting the same pairing code.			
cisco -- mx011anm_firmware	The Comcast firmware on Motorola MX011ANM (firmware version MX011AN_2.9p6s1_PROD_sey) devices allows physically proximate attackers to access an SNMP server by connecting a cable to the Ethernet port, and then establishing communication with the device's link-local IPv6 address.	2017-07-30	4.6	CVE-2017-9496 MISC(link is external)
connectwise -- manage	services/system_io/actionprocessor/System.rails in ConnectWise Manage 2017.5 is vulnerable to Cross-Site Request Forgery (CSRF), as demonstrated by changing an e-mail address setting.	2017-07-31	6.8	CVE-2017-11726 MISC(link is external)
connectwise -- manage	services/system_io/actionprocessor/Contact.rails in ConnectWise Manage 2017.5 allows arbitrary client-side JavaScript code execution (involving a ContactCommon field) on victims who click on a crafted link, aka XSS.	2017-07-31	4.3	CVE-2017-11727 MISC(link is external)
earcms -- ear_music	In Earcms Ear Music through 4.1 build 20170710, remote authenticated users can execute arbitrary PHP code by changing the allowable music-upload extensions to include .php in addition to .mp3 and .m4a in admin.php?iframe=config_upload, and then using user.php/music/add/ to upload the code.	2017-07-30	6.0	CVE-2017-11756 MISC(link is external)
ffmpeg -- ffmpeg	The dnxhd_decode_header function in libavcodec/dnxhddec.c in FFmpeg through 3.3.2 allows remote attackers to cause a denial of service (out-of-array access) or possibly have unspecified other impact via a crafted DNxHD file.	2017-07-28	6.8	CVE-2017-11719 BID(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gigaccsecure -- gigacc_office	GigaCC OFFICE ver.2.3 and earlier allows remote attackers to execute arbitrary OS commands via specially crafted mail template.	2017-08-02	6.0	CVE-2016-7844 BID(link is external) MISC(link is external) MISC(link is external)
gigaccsecure -- gigacc_office	GigaCC OFFICE ver.2.3 and earlier allows remote attackers to upload arbitrary files as a user profile image, which may be exploited for unauthorized file sharing.	2017-08-02	5.5	CVE-2016-7845 BID(link is external) MISC(link is external) MISC(link is external)
gitlab -- gitlab	GitLab Enterprise Edition (EE) before 8.17.7, 9.0.11, 9.1.8, 9.2.8, and 9.3.8 allows an authenticated user with the ability to create a project to use the mirroring feature to potentially read repositories belonging to other users.	2017-08-02	4.0	CVE-2017-11437 CONFIRM(link is external)
gnu -- glibc	The DNS stub resolver in the GNU C Library (aka glibc or libc6) before version 2.26, when EDNS support is enabled, will solicit large UDP responses from name servers, potentially simplifying off-path DNS spoofing attacks due to IP fragmentation.	2017-08-01	4.3	CVE-2017-12132 MISC MISC
graphicsmagick -- graphicsmagick	The WriteOnePNGImage function in coders/png.c in GraphicsMagick 1.3.26 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted file, because the program's actual control flow was inconsistent with its indentation. This resulted in a logging statement executing outside of a loop, and consequently using an	2017-07-28	4.3	CVE-2017-11722 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	invalid array index corresponding to the loop's exit condition.			
ibm -- api_connect	IBM API Connect 5.0.0.0 could allow a user to bypass policy restrictions and create non-compliant passwords which could be intercepted and decrypted using man in the middle techniques. IBM X-Force ID: 127160.	2017-07-31	4.3	CVE-2017-1386 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- i	IBM i OSPF 6.1, 7.1, 7.2, and 7.3 is vulnerable when a rogue router spoofs its origin. Routing tables are affected by a missing LSA, which may lead to loss of connectivity. IBM X-Force ID: 128379.	2017-07-31	5.0	CVE-2017-1460 MISC(link is external) MISC(link is external)
ibm -- infosphere_information_server	IBM InfoSphere Information Server 9.1, 11.3, and 11.5 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 127155.	2017-08-02	6.4	CVE-2017-1383 CONFIRM(link is external) MISC(link is external)
ibm -- infosphere_information_server	A network layer security vulnerability in InfoSphere Information Server 9.1, 11.3, and 11.5 can lead to privilege escalation or unauthorized access. IBM X-Force ID: 128466.	2017-08-02	6.8	CVE-2017-1467 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- infosphere_information_server	IBM InfoSphere Information Server 9.1, 11.3, and 11.5 could allow a local user to gain elevated privileges by placing arbitrary files in installation directories. IBM X-force ID: 128467.	2017-08-02	4.6	CVE-2017-1468 CONFIRM(link is external) BID(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				external) MISC(link is external)
ibm -- infosphere_information_server	IBM InfoSphere Information Server 9.1, 11.3, and 11.5 could allow a privileged user to cause a memory dump that could contain highly sensitive information including access credentials. IBM X-Force ID: 128693.	2017-08-02	4.0	CVE-2017-1495 CONFIRM(link is external) MISC(link is external)
ibm -- infosphere_master_data_management_server	IBM InfoSphere Master Data Management Server 10.1, 11.0, 11.3, 11.4, 11.5, and 11.6 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: 119727.	2017-07-31	6.8	CVE-2016-9714 CONFIRM(link is external) MISC(link is external)
ibm -- infosphere_master_data_management_server	IBM InfoSphere Master Data Management Server 11.0, 11.3, 11.4, 11.5, and 11.6 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: 119729.	2017-07-31	6.8	CVE-2016-9716 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- infosphere_master_data_management_server	HTTP Parameter Override is identified in the IBM Infosphere Master Data Management (MDM) 10.1. 11.0. 11.3, 11.4, 11.5, and 11.6 product. It enables attackers by exposing the presence of duplicated parameters which may produce an anomalous behavior in the application that can be potentially exploited.	2017-07-31	4.0	CVE-2016-9717 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- inotes	IBM iNotes 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web	2017-08-03	4.3	CVE-2017-1327 CONFIRM(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 126062.			external) BID(link is external) MISC(link is external)
ibm -- inotes	IBM iNotes 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 126234.	2017-07-31	4.3	CVE-2017-1332 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- jazz_reporting_service	IBM Jazz Reporting Service (JRS) 5.0 and 6.0 could disclose sentive information, including user credentials, through an error message from the Report Builder administrator configuration page. IBM X-Force ID: 126863.	2017-07-31	4.0	CVE-2017-1370 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- mobilefirst_platform_foundation	A Reflected Cross Site Scripting (XSS) vulnerability exists in the authorization function exposed by RESTful Web Api of IBM Worklight Framework 6.1, 6.2, 6.3, 7.0, 7.1, and 8.0. The vulnerable parameter is "scope"; if you set as its value a "realm" not defined in authenticationConfig.xml, you get an HTTP 403 Forbidden response and the value will be reflected in the body of the HTTP response. By setting it to arbitrary JavaScript code it is possible to modify the flow of the authorization function, potentially leading to credential disclosure within a trusted session.	2017-08-01	4.3	CVE-2017-1500 CONFIRM(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- websphere_application_server	IBM WebSphere Application Server version 9.0.0.4 could provide weaker than expected security after using the PasswordUtil command to enable AES password encryption. IBM X-Force ID: 129579.	2017-08-03	4.0	CVE-2017-1504 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- websphere_mq_internet_pass-thru	IBM WebSphere MQ Internet Pass-Thru 2.0 and 2.1 could allow n attacker to cause the MQIPT to stop responding due to an incorrectly configured security policy. IBM X-Force ID: 121156.	2017-08-02	5.0	CVE-2017-1118 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- websphere_portal	IBM WebSphere Portal and Web Content Manager 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 125457.	2017-07-31	4.3	CVE-2017-1303 CONFIRM(link is external) BID(link is external) MISC(link is external)
iid -- rbb_speed_test	The RBB SPEED TEST App for Android version 2.0.3 and earlier, RBB SPEED TEST App for iOS version 2.1.0 and earlier does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2017-08-02	4.3	CVE-2017-2278 MISC(link is external) JVN(link is external)
imagemagick -- imagemagick	The ReadMATImage function in coders/mat.c in ImageMagick through 6.9.9-3 and 7.x through 7.0.6-3 has memory leaks involving the	2017-07-29	4.3	CVE-2017-11724 CONFIRM(li

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	quantum_info and clone_info data structures.			nk is external)
imagemagick -- imagemagick	The ReadOneJNGImage function in coders/png.c in ImageMagick 6.9.9-4 and 7.0.6-4 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.	2017-07-30	4.3	CVE-2017-11750 CONFIRM(link is external)
imagemagick -- imagemagick	The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file.	2017-07-30	4.3	CVE-2017-11751 CONFIRM(link is external)
imagemagick -- imagemagick	The ReadMAGICKImage function in coders/magick.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file.	2017-07-30	4.3	CVE-2017-11752 CONFIRM(link is external)
imagemagick -- imagemagick	The GetImageDepth function in MagickCore/attribute.c in ImageMagick 7.0.6-4 might allow remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted Flexible Image Transport System (FITS) file.	2017-07-30	4.3	CVE-2017-11753 MISC(link is external)
imagemagick -- imagemagick	The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file that is mishandled in an OpenPixelCache call.	2017-07-30	4.3	CVE-2017-11754 MISC(link is external)
imagemagick -- imagemagick	The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file that is mishandled in an AcquireSemaphoreInfo call.	2017-07-30	4.3	CVE-2017-11755 MISC(link is external)
imagemagick -- imagemagick	ImageMagick 7.0.6-5 has memory leaks in the parse8BIMW and	2017-08-03	5.0	CVE-2017-12418

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	format8BIM functions in coders/meta.c, related to the WriteImage function in MagickCore/constitute.c.			CONFIRM(link is external)
imagemagick -- imagemagick	The ProcessMSLScript function in coders/msl.c in ImageMagick before 6.9.9-5 and 7.x before 7.0.6-5 allows remote attackers to cause a denial of service (memory leak) via a crafted file, related to the WriteMSLImage function.	2017-08-04	4.3	CVE-2017-12427 CONFIRM(link is external) CONFIRM(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.6-1, a memory leak vulnerability was found in the function ReadWMFImage in coders/wmf.c, which allows attackers to cause a denial of service in CloneDrawInfo in draw.c.	2017-08-04	5.0	CVE-2017-12428 CONFIRM(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.6-1, a use-after-free vulnerability was found in the function ReadWMFImage in coders/wmf.c, which allows attackers to cause a denial of service.	2017-08-04	4.3	CVE-2017-12431 CONFIRM(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.6-1, a memory leak vulnerability was found in the function ReadPESImage in coders/pes.c, which allows attackers to cause a denial of service, related to ResizeMagickMemory in memory.c.	2017-08-04	4.3	CVE-2017-12433 CONFIRM(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.6-1, a missing NULL check vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service (assertion failure) in DestroyImageInfo in image.c.	2017-08-04	4.3	CVE-2017-12434 CONFIRM(link is external)
joomla -- joomla!	The CMS installer in Joomla! before 3.7.4 does not verify a user's ownership of a webspace, which	2017-08-02	6.5	CVE-2017-11364 SECTRACK(

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows remote authenticated users to gain control of the target application by leveraging Certificate Transparency logs.			link is external) CONFIRM MISC MISC(link is external)
libid3tag_project -- libid3tag	The id3_ucs4_length function in ucs4.c in libid3tag 0.15.1b allows remote attackers to cause a denial of service (NULL Pointer Dereference and application crash) via a crafted mp3 file.	2017-07-31	4.3	CVE-2017-11550 MISC
libid3tag_project -- libid3tag	The id3_field_parse function in field.c in libid3tag 0.15.1b allows remote attackers to cause a denial of service (OOM) via a crafted MP3 file.	2017-07-31	4.3	CVE-2017-11551 MISC
libming -- ming	A memory leak vulnerability was found in the function parseSWF_DOACTION in util/parser.c in Ming 0.4.8, which allows attackers to cause a denial of service via a crafted file.	2017-07-28	4.3	CVE-2017-11703 MISC(link is external) MISC(link is external)
libming -- ming	A heap-based buffer over-read was found in the function decompileIF in util/decompile.c in Ming 0.4.8, which allows attackers to cause a denial of service via a crafted file.	2017-07-28	4.3	CVE-2017-11704 MISC(link is external) MISC(link is external)
libming -- ming	A memory leak was found in the function parseSWF_SHAPEWITHSTYLE in util/parser.c in Ming 0.4.8, which allows attackers to cause a denial of service via a crafted file.	2017-07-28	4.3	CVE-2017-11705 MISC(link is external) MISC(link is external)
libming -- ming	A heap-based buffer over-read was found in the function OpCode (called from decompileSETMEMBER) in util/decompile.c in Ming 0.4.8, which	2017-07-29	4.3	CVE-2017-11728 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows attackers to cause a denial of service via a crafted file.			MISC(link is external)
libming -- ming	A heap-based buffer over-read was found in the function OpCode (called from decompileINCR_DECR line 1440) in util/decompile.c in Ming 0.4.8, which allows attackers to cause a denial of service via a crafted file.	2017-07-29	4.3	CVE-2017-11729 MISC(link is external) MISC(link is external)
libming -- ming	A heap-based buffer over-read was found in the function OpCode (called from decompileINCR_DECR line 1474) in util/decompile.c in Ming 0.4.8, which allows attackers to cause a denial of service via a crafted file.	2017-07-29	4.3	CVE-2017-11730 MISC(link is external) MISC(link is external)
libming -- ming	An invalid memory read vulnerability was found in the function OpCode (called from isLogicalOp and decompileIF) in util/decompile.c in Ming 0.4.8, which allows attackers to cause a denial of service via a crafted file.	2017-07-29	4.3	CVE-2017-11731 MISC(link is external) MISC(link is external)
libming -- ming	A heap-based buffer overflow vulnerability was found in the function dcputs (called from decompileIMPLEMENTS) in util/decompile.c in Ming 0.4.8, which allows attackers to cause a denial of service via a crafted file.	2017-07-29	4.3	CVE-2017-11732 MISC(link is external) MISC(link is external)
libming -- ming	A null pointer dereference vulnerability was found in the function stackswap (called from decompileSTACKSWAP) in util/decompile.c in Ming 0.4.8, which allows attackers to cause a denial of service via a crafted file.	2017-07-29	4.3	CVE-2017-11733 MISC(link is external) MISC(link is external)
libming -- ming	A heap-based buffer over-read was found in the function decompileCALLFUNCTION in util/decompile.c in Ming 0.4.8, which	2017-07-29	4.3	CVE-2017-11734 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows attackers to cause a denial of service via a crafted file.			MISC(link is external)
libquicktime -- libquicktime	In libquicktime 1.2.4, an allocation failure was found in the function quicktime_read_info in lqt_quicktime.c, which allows attackers to cause a denial of service via a crafted file.	2017-08-02	4.3	CVE-2017-12143 MISC(link is external) MISC(link is external)
libquicktime -- libquicktime	In libquicktime 1.2.4, an allocation failure was found in the function quicktime_read_ftyp in ftyp.c, which allows attackers to cause a denial of service via a crafted file.	2017-08-02	4.3	CVE-2017-12145 MISC(link is external) MISC(link is external)
microsoft -- outlook	Microsoft Outlook 2007 SP3, Outlook 2010 SP2, Outlook 2013 SP1, Outlook 2013 RT SP1, and Outlook 2016 as packaged in Microsoft Office allows a security feature bypass vulnerability due to the way that it handles input, aka "Microsoft Office Outlook Security Feature Bypass Vulnerability".	2017-08-01	6.8	CVE-2017-8571 BID(link is external) SECTRACK(link is external) CONFIRM(link is external)
microsoft -- outlook	Microsoft Outlook 2007 SP3, Outlook 2010 SP2, Outlook 2013 SP1, Outlook 2013 RT SP1, and Outlook 2016 as packaged in Microsoft Office allows an information disclosure vulnerability due to the way that it discloses the contents of its memory, aka "Microsoft Office Outlook Information Disclosure Vulnerability".	2017-08-01	4.3	CVE-2017-8572 BID(link is external) SECTRACK(link is external) CONFIRM(link is external)
modx -- modx_revolution	In MODX Revolution 2.5.7, the "key" and "name" parameters in the System Settings module are vulnerable to XSS. A malicious payload sent to connectors/index.php will be triggered	2017-07-30	4.3	CVE-2017-11744 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	by every user, when they visit this module.			
motorola -- mx011anm_firmware	The Comcast firmware on Motorola MX011ANM (firmware version MX011AN_2.9p6s1_PROD_sey) devices allows remote attackers to enable a Remote Web Inspector that is accessible from the public Internet.	2017-07-30	5.0	CVE-2017-9494 MISC(link is external)
netcomm -- 4gt101w_bootloader	NetComm Wireless 4GT101W routers with Hardware: 0.01 / Software: V1.1.8.8 / Bootloader: 1.1.3 are vulnerable to CSRF attacks, as demonstrated by using administration.html to disable the firewall. They does not contain any token that can mitigate CSRF vulnerabilities within the device.	2017-07-28	6.8	CVE-2017-11646 MISC(link is external)
nvidia -- gpu_driver	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where a value passed from a user to the driver is not correctly validated and used as the index to an array which may lead to denial of service or potential escalation of privileges.	2017-07-28	4.6	CVE-2017-6256 CONFIRM(link is external)
open-emr -- openemr	The csv_log_html function in library/edihistory/edih_csv_inc.php in OpenEMR 5.0.0 and prior allows attackers to bypass intended access restrictions via a crafted name.	2017-08-01	5.0	CVE-2017-12064 CONFIRM(link is external)
openexif_project -- openexif	The ExifJpegHUFFTable::deriveTable function in ExifHuffmanTable.cpp in OpenExif 2.1.4 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) via a crafted jpg file.	2017-07-31	4.3	CVE-2017-11115 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openexif_project -- openexif	The ExifImageFile::readDQT function in ExifImageFileRead.cpp in OpenExif 2.1.4 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted jpg file.	2017-07-31	6.8	CVE-2017-11116 MISC
openexif_project -- openexif	The ExifImageFile::readDHT function in ExifImageFileRead.cpp in OpenExif 2.1.4 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted jpg file.	2017-07-31	4.3	CVE-2017-11117 MISC
paloaltonetworks -- pan-os	Cross-site scripting (XSS) vulnerability in the management web interface in Palo Alto Networks PAN-OS before 6.1.18, 7.x before 7.0.16, 7.1.x before 7.1.11, and 8.x before 8.0.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-08-02	4.3	CVE-2017-9459 BID(link is external) SECTRACK(link is external) CONFIRM(link is external)
paloaltonetworks -- pan-os	Cross-site scripting (XSS) vulnerability in the GlobalProtect external interface in Palo Alto Networks PAN-OS before 6.1.18, 7.x before 7.0.16, 7.1.x before 7.1.11, and 8.x before 8.0.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-08-02	4.3	CVE-2017-9467 BID(link is external) SECTRACK(link is external) CONFIRM(link is external)
pega -- pega_platform	Multiple cross-site scripting (XSS) vulnerabilities in PEGA Platform 7.2 ML0 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) PATH_INFO to the main page; the (2) beanReference	2017-08-02	4.3	CVE-2017-11355 FULLDISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameter to the JavaBean viewer page; or the (3) pyTableName to the System database schema modification page.			
pega -- pega_platform	The application distribution export functionality in PEGA Platform 7.2 ML0 and earlier allows remote authenticated users with certain privileges to obtain sensitive configuration information by leveraging a missing access control.	2017-08-02	4.0	CVE-2017-11356 FULLDISC
qemu -- qemu	qemu-nbd in QEMU (aka Quick Emulator) does not ignore SIGPIPE, which allows remote attackers to cause a denial of service (daemon crash) by disconnecting during a server-to-client reply attempt.	2017-08-02	5.0	CVE-2017-10664 MLIST(link is external) BID(link is external) MISC(link is external) MLIST
rspamd_project -- rspamd	interface/js/app/history.js in WebUI in Rspamd before 1.6.3 allows XSS via the Subject and Message-Id headers, which are mishandled in the history page.	2017-07-29	4.3	CVE-2017-11737 CONFIRM(link is external) CONFIRM(link is external)
samsung -- samsung_mobile	Race condition in the ioctl implementation in the Samsung Graphics 2D driver (aka /dev/fimg2d) in Samsung devices with Android L(5.0/5.1) allows local users to trigger memory errors by leveraging definition of g2d_lock and g2d_unlock lock macros as no-ops, aka SVE-2015-4598.	2017-08-02	4.4	CVE-2015-7891 MISC(link is external) CONFIRM(link is external) BID(link is external) MISC EXPLOIT-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				DB(link is external)
silkypress -- simple_custom_css_and_js	Cross-site scripting vulnerability in Simple Custom CSS and JS prior to version 3.4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-08-02	4.3	CVE-2017-2285 JVN(link is external) MISC MISC MISC(link is external)
sound_exchange_project -- sound_exchange	The startread function in wav.c in Sound eXchange (SoX) 14.4.2 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted wav file.	2017-07-31	4.3	CVE-2017-11332 MISC
sound_exchange_project -- sound_exchange	The read_samples function in hcom.c in Sound eXchange (SoX) 14.4.2 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted hcom file.	2017-07-31	4.3	CVE-2017-11358 MISC
sound_exchange_project -- sound_exchange	The wavwritehdr function in wav.c in Sound eXchange (SoX) 14.4.2 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted snd file, during conversion to a wav file.	2017-07-31	4.3	CVE-2017-11359 MISC
techroutes -- tr_1803-3g_firmware	Techroutes TR 1803-3G Wireless Cellular Router/Modem 2.4.25 devices do not possess any protection against a CSRF vulnerability, as demonstrated by a goform/BasicSettings request to disable port filtering.	2017-07-31	6.8	CVE-2017-11648 MISC(link is external)
timidity++_project -- timidity++	The insert_note_steps function in readmidi.c in TiMidity++ 2.14.0 allows remote attackers to cause a denial of service (divide-by-zero error	2017-07-31	4.3	CVE-2017-11546 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and application crash) via a crafted mid file. NOTE: a crash might be relevant when using the --background option.			
timidity++_project -- timidity++	The resample_gauss function in resample.c in TiMidity++ 2.14.0 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted mid file. NOTE: a crash might be relevant when using the --background option. NOTE: the TiMidity++ README.alsaseq documentation suggests a setuid-root installation.	2017-07-31	4.3	CVE-2017-11547 MISC
trendmicro -- control_manager	Authentication Bypass in Trend Micro Control Manager 6.0 causes Information Disclosure when authentication validation is not done for functionality that can change debug logging level. Formerly ZDI-CAN-4512.	2017-08-02	5.0	CVE-2017-11387 BID(link is external) SECTRACK(link is external) MISC(link is external) MISC(link is external)
trendmicro -- control_manager	SQL Injection in Trend Micro Control Manager 6.0 causes Remote Code Execution when RestfulServiceUtility.NET.dll doesn't properly validate user provided strings before constructing SQL queries. Formerly ZDI-CAN-4639 and ZDI-CAN-4638.	2017-08-02	6.5	CVE-2017-11388 BID(link is external) SECTRACK(link is external) MISC(link is external) MISC(link is external) MISC(link is external)
trendmicro -- control_manager	XML external entity (XXE) processing vulnerability in Trend	2017-08-02	5.0	CVE-2017-11390

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Micro Control Manager 6.0, if exploited, could lead to information disclosure. Formerly ZDI-CAN-4706.			BID(link is external) MISC(link is external) MISC(link is external)
trendmicro -- deep_discovery_email_inspector	Denial of Service vulnerability in Trend Micro Deep Discovery Email Inspector 2.5.1 allows remote attackers to delete arbitrary files on vulnerable installations, thus disabling the service. Formerly ZDI-CAN-4350.	2017-08-03	6.4	CVE-2017-11382 BID(link is external) MISC(link is external) MISC(link is external)
trendmicro -- interscan_messaging_security_virtual_appliance	Proxy command injection vulnerability in Trend Micro InterScan Messaging Virtual Appliance 9.0 and 9.1 allows remote attackers to execute arbitrary code on vulnerable installations. The specific flaw can be exploited by parsing the "T" parameter within modTMCSS Proxy. Formerly ZDI-CAN-4745.	2017-08-03	6.5	CVE-2017-11392 BID(link is external) MISC(link is external) MISC(link is external)
vmware -- vcenter_server	VMware vCenter Server (6.5 prior to 6.5 U1) contains an insecure library loading issue that occurs due to the use of LD_LIBRARY_PATH variable in an unsafe manner. Successful exploitation of this issue may allow unprivileged host users to load a shared library that may lead to privilege escalation.	2017-08-01	6.5	CVE-2017-4921 BID(link is external) SECTRACK(link is external) CONFIRM(link is external)
vmware -- vcenter_server	VMware vCenter Server (6.5 prior to 6.5 U1) contains an information disclosure issue due to the service startup script using world writable directories as temporary storage for critical information. Successful exploitation of this issue may allow	2017-08-01	4.0	CVE-2017-4922 BID(link is external) SECTRACK(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unprivileged host users to access certain critical information when the service gets restarted.			CONFIRM(link is external)
vmware -- vcenter_server	VMware vCenter Server (6.5 prior to 6.5 U1) contains an information disclosure vulnerability. This issue may allow plaintext credentials to be obtained when using the vCenter Server Appliance file-based backup feature.	2017-08-01	5.0	CVE-2017-4923 BID(link is external) SECTRACK(link is external) CONFIRM(link is external)
wppopupmaker -- popup_maker	Cross-site scripting vulnerability in Popup Maker prior to version 1.6.5 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-08-02	4.3	CVE-2017-2284 JVN(link is external) MISC MISC
xinha -- xinha	Directory traversal vulnerability in plugins/ImageManager/backend.php in Xinha 0.96, as used in Jojo 4.4.0, allows remote attackers to delete any folder via directory traversal sequences in the deld parameter.	2017-07-29	5.0	CVE-2017-11723 CONFIRM(link is external)
xiph.org -- libao	The _tokenize_matrix function in audio_out.c in Xiph.Org libao 1.2.0 allows remote attackers to cause a denial of service (memory corruption) via a crafted MP3 file.	2017-07-31	4.3	CVE-2017-11548 MISC
xiph.org -- libvorbis	The vorbis_analysis_wrote function in lib/block.c in Xiph.Org libvorbis 1.3.5 allows remote attackers to cause a denial of service (OOM) via a crafted wav file.	2017-07-31	4.3	CVE-2017-11333 MISC
xiph.org -- libvorbis	The vorbis_block_clear function in lib/block.c in Xiph.Org libvorbis 1.3.5 allows remote attackers to cause a denial of service (NULL pointer	2017-07-31	4.3	CVE-2017-11735 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	dereference and application crash) via a crafted ogg file.			
xiph.org -- vorbis-tools	The wav_open function in oggenc/audio.c in Xiph.Org vorbis-tools 1.4.0 allows remote attackers to cause a denial of service (memory allocation error) via a crafted wav file.	2017-07-31	4.3	CVE-2017-11331 MISC
xoops -- xoops	XOOPS Core 2.5.8 has a stored URL redirect bypass vulnerability in /modules/profile/index.php because of the URL filter.	2017-08-02	5.8	CVE-2017-12138 BID(link is external) CONFIRM(link is external)
xoops -- xoops	XOOPS Core 2.5.8 has stored XSS in imagemanager.php because of missing MIME type validation in htdocs/class/uploader.php.	2017-08-02	4.3	CVE-2017-12139 BID(link is external) CONFIRM(link is external)
ytnef_project -- ytnef	In ytnef 1.9.2, a heap-based buffer overflow vulnerability was found in the function TNEFFillMapi in ytnef.c, which allows attackers to cause a denial of service via a crafted file.	2017-08-02	4.3	CVE-2017-12141 MISC(link is external) MISC(link is external)
ytnef_project -- ytnef	In ytnef 1.9.2, an invalid memory read vulnerability was found in the function SwapDWord in ytnef.c, which allows attackers to cause a denial of service via a crafted file.	2017-08-02	4.3	CVE-2017-12142 MISC(link is external) MISC(link is external)
ytnef_project -- ytnef	In ytnef 1.9.2, an allocation failure was found in the function TNEFFillMapi in ytnef.c, which allows attackers to cause a denial of service via a crafted file.	2017-08-02	4.3	CVE-2017-12144 BID(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC(link is external)

Back to top

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
cacti -- cacti	Cross-site scripting (XSS) vulnerability in aggregate_graphs.php in Cacti before 1.1.16 allows remote authenticated users to inject arbitrary web script or HTML via specially crafted HTTP Referer headers, related to the $cancel_url variable. NOTE: this vulnerability exists because of an incomplete fix (lack of the htmlspecialchars ENT_QUOTES flag) for CVE-2017-11163.	2017-08-01	3.5	CVE-2017-12066 CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421733-160420a-CMCST); Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST); and Arris TG1682G (eMTA&DOCSIS version 10.0.132.SIP.PC20.CT, software version TG1682_2.2p7s2_PROD_sey) devices makes it easy for remote attackers to determine the hidden SSID and passphrase for a Home Security Wi-Fi network.	2017-07-30	3.3	CVE-2017-9476 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421733-160420a-CMCST) and DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST) devices allows remote attackers to discover the CM MAC address by connecting to the device's xfinitywifi hotspot.	2017-07-30	3.3	CVE-2017-9477 MISC(link is external)
cisco -- dpc3939_firmware	The Comcast firmware on Cisco DPC3939 (firmware version dpc3939-P20-18-v303r20421746-170221a-CMCST) devices allows local users (e.g., users who have command access as a consequence of CVE-2017-9479 exploitation) to read arbitrary files via UPnP access to /var/IGD/.	2017-07-30	2.1	CVE-2017-9480 MISC(link is external)
comcast -- xfinity_xr11-20_firmware	The Comcast firmware on Motorola MX011ANM (firmware version MX011AN_2.9p6s1_PROD_sey) and Xfinity XR11-20 Voice Remote devices allows local users to upload arbitrary firmware images to an XR11 by leveraging root access. In other words, there is no protection mechanism involving digital signatures for the firmware.	2017-07-30	2.1	CVE-2017-9498 MISC(link is external)
ibm -- infosphere_master_data_management_server	IBM InfoSphere Master Data Management Server 11.0, 11.3, 11.4, 11.5, and 11.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary	2017-07-31	3.5	CVE-2016-9715 CONFIRM(link is external) BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 119728.			MISC(link is external)
ibm -- infosphere_master_data_management_server	IBM InfoSphere Master Data Management Server 10.1. 11.0. 11.3, 11.4, 11.5, and 11.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 119732.	2017-07-31	3.5	CVE-2016-9718 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- infosphere_master_data_management_server	IBM InfoSphere Master Data Management Server 10.1. 11.0. 11.3, 11.4, 11.5, and 11.6 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 119733.	2017-07-31	3.5	CVE-2016-9719 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- infosphere_master_data_management_server	IBM InfoSphere Master Data Management Server 10.0, 11.0, 11.3, 11.4, 11.5, and 11.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially	2017-08-03	3.5	CVE-2017-1199 CONFIRM(link is external) BID(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	leading to credentials disclosure within a trusted session. IBM X-Force ID: 123674.			
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 5.2.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: 128694.	2017-07-31	3.5	CVE-2017-1496 CONFIRM(link is external) MISC(link is external)
motorola -- mx011anm_firmware	The Comcast firmware on Motorola MX011ANM (firmware version MX011AN_2.9p6s1_PROD_sey) devices allows physically proximate attackers to read arbitrary files by pressing "EXIT, Down, Down, 2" on an RF4CE remote to reach the diagnostic display, and then launching a Remote Web Inspector script.	2017-07-30	2.1	CVE-2017-9495 MISC(link is external)
netcomm -- 4gt101w_bootloader	NetComm Wireless 4GT101W routers with Hardware: 0.01 / Software: V1.1.8.8 / Bootloader: 1.1.3 are vulnerable to stored cross-site scripting attacks. Creating an SSID with an XSS payload results in successful exploitation.	2017-07-28	3.5	CVE-2017-11647 MISC(link is external)
qemu -- qemu	Stack-based buffer overflow in hw/usb/redirect.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a	2017-08-02	2.1	CVE-2017-10806 MLIST(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	denial of service (QEMU process crash) via vectors related to logging debug messages.			BID(link is external) CONFIRM(link is external) MLIST
qemu -- qemu	The address_space_write_continue function in exec.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (out-of-bounds access and guest instance crash) by leveraging use of qemu_map_ram_ptr to access guest ram block area.	2017-08-02	2.1	CVE-2017-11334 MLIST(link is external) BID(link is external) CONFIRM(link is external) MLIST
tinyproxy_project -- tinyproxy	main.c in Tinyproxy 1.8.4 and earlier creates a /run/tinyproxy/tinyproxy.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 tinyproxy.pid modification before a root script executes a "kill `cat /run/tinyproxy/tinyproxy.pid`" command.	2017-07-30	2.1	CVE-2017-11747 MISC(link is external)

Back to top

Severity Not Yet Assigned				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
axis_communications -- axis_2100_devices	AXIS 2100 devices 2.43 have XSS via the URI, possibly related to admin/admin.shtml.	2017-08-04	not yet calculated	CVE-2017-12413 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
baidu_japan -- baidu_ime	Untrusted search path vulnerability in Installer of Baidu IME Ver3.6.1.6 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-08-04	not yet calculated	CVE-2017-2221 JVN(link is external)
bank_of_tokyo-mitsubishi_ufj -- bank_of_tokyo-mitsubishi_ufj_app	The Bank of Tokyo-Mitsubishi UFJ, Ltd. App for Android ver5.3.1, ver5.2.2 and earlier allow a man-in-the-middle attacker to downgrade the communication between the app and the server from TLS v1.2 to SSL v3.0, which may result in the attacker to eavesdrop on an encrypted communication.	2017-08-02	not yet calculated	CVE-2016-7812 BID(link is external) MISC(link is external)
brother_industries -- dcp_printers	Denial of Service vulnerability in Debut embedded httpd 1.20 in Brother DCP-J132W (and probably other DCP models) allows remote attackers to hang the printer (disrupting its network connection) by sending a large amount of HTTP packets.	2017-08-05	not yet calculated	CVE-2017-12568 MISC(link is external)
citrix -- netscaler_devices	The TLS and DTLS processing functionality in Citrix NetScaler Application Delivery Controller (ADC) and NetScaler Gateway devices with firmware 9.x before 9.3 Build 68.5, 10.0 through Build 78.6, 10.1 before Build 130.13, 10.1.e before Build 130.1302.e, 10.5 before Build 55.8, and 10.5.e before Build 55.8007.e makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, a variant of CVE-2014-3566 (aka POODLE).	2017-08-02	not yet calculated	CVE-2015-3642 CONFIRM(link is external)
claybird -- lhhaforge	Untrusted search path vulnerability in LhaForge Ver.1.6.5 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-08-02	not yet calculated	CVE-2017-2288 JVN(link is external)
comcast -- arris_tg1682g_devices	The Comcast firmware on Arris TG1682G (eMTA&DOCSIS version 10.0.132.SIP.PC20.CT, software version TG1682_2.2p7s2_PROD_sey) devices allows configuration changes via CSRF.	2017-07-30	not yet calculated	CVE-2017-9490 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
comcast -- xfinity_wifi_home_hotspot	Comcast XFINITY WiFi Home Hotspot devices allow remote attackers to spoof the identities of Comcast customers via a forged MAC address.	2017-07-30	not yet calculated	CVE-2017-9475 MISC(link is external)
dashlane -- dashlane	Dashlane might allow local users to gain privileges by placing a Trojan horse WINHTTP.dll in the %APPDATA%\Dashlane directory.	2017-08-04	not yet calculated	CVE-2017-11657 MISC(link is external)
dell -- storage_manager_2016	Directory Traversal in Dell Storage Manager 2016 R2.1 causes Information Disclosure when the doGet method of the EmWebsiteServlet class doesn't properly validate user provided path before using it in file operations. Was ZDI-CAN-4459.	2017-08-04	not yet calculated	CVE-2017-10949 MISC(link is external) BID(link is external) MISC(link is external)
divfix++ -- divfix++	The DivFixppCore::avi_header_fix function in DivFix++Core.cpp in DivFix++ v0.34 allows remote attackers to cause a denial of service (invalid memory write and application crash) via a crafted avi file.	2017-07-31	not yet calculated	CVE-2017-11330 MISC
dokuwiki -- dokuwiki	DokuWiki through 2017-02-19b has XSS in the at parameter (aka the DATE_AT variable) to doku.php.	2017-08-05	not yet calculated	CVE-2017-12583 CONFIRM(link is external)
expat -- expat	The writeRandomBytes_RtlGenRandom function in xmlparse.c in libexpat in Expat 2.2.1 and 2.2.2 on Windows allows local users to gain privileges via a Trojan horse ADVAPI32.DLL in the current working directory because of an untrusted search path, aka DLL hijacking.	2017-07-30	not yet calculated	CVE-2017-11742 CONFIRM(link is external)
f-secure_online_scanner -- f-secure_online_scanner	Untrusted search path vulnerability in F-Secure Online Scanner allows remote attackers to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse DLL that is located in the same folder as F-SecureOnlineScanner.exe.	2017-08-02	not yet calculated	CVE-2015-8264 FULLDISC BUGTRAQ(link is external) BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM(link is external)
freetime -- formatfactory	FormatFactory 4.1.0 has a DLL Hijacking Vulnerability because an untrusted search path is used for msimg32.dll, WindowsCodecs.dll, and dwmapi.dll.	2017-08-03	not yet calculated	CVE-2017-12414 MISC(link is external)
frogman_office -- cs-cart	Cross-site request forgery (CSRF) vulnerability in CS-Cart Japanese Edition v4.3.10 and earlier (excluding v2 and v3), CS-Cart Multivendor Japanese Edition v4.3.10 and earlier (excluding v2 and v3) allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2017-08-02	not yet calculated	CVE-2017-2138 MISC(link is external) JVN(link is external)
github_inc -- electron	GitHub Electron before 1.6.8 allows remote command execution because of a nodeIntegration bypass vulnerability. This also affects all applications that bundle Electron code equivalent to 1.6.8 or earlier. Bypassing the Same Origin Policy (SOP) is a precondition; however, recent Electron versions do not have strict SOP enforcement. Combining an SOP bypass with a privileged URL internally used by Electron, it was possible to execute native Node.js primitives in order to run OS commands on the user's host. Specifically, a chrome-devtools://devtools/bundled/inspector.html window could be used to eval a Node.js child_process.execFile API call.	2017-08-05	not yet calculated	CVE-2017-12581 MISC(link is external)
gitlab -- community_and_enterprise_editions	GitLab Community Edition (CE) and Enterprise Edition (EE) before 9.0.11, 9.1.8, 9.2.8 allow an authenticated user with the ability to create a group to add themselves to any project that is inside a subgroup.	2017-08-02	not yet calculated	CVE-2017-11438 CONFIRM(link is external)
gnu_binutils -- gnu_binutils	The bfd_mach_o_i386_canonicalize_one_reloc function in bfd/mach-o-i386.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29	2017-08-04	not yet calculated	CVE-2017-12452 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and earlier, allows remote attackers to cause an out of bounds heap read via a crafted mach-o file.			
gnu_binutils -- gnu_binutils	The bfd_make_section_with_flags function in section.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause a NULL dereference via a crafted file.	2017-08-04	not yet calculated	CVE-2017-12457 MISC
gnu_binutils -- gnu_binutils	The read_symbol_stabs_debugging_info function in rddbg.c in GNU Binutils 2.29 and earlier allows remote attackers to cause an out of bounds heap read via a crafted binary file.	2017-08-04	not yet calculated	CVE-2017-12456 MISC
gnu_binutils -- gnu_binutils	The nlm_swap_auxiliary_headers_in function in bfd/nlmcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted nlm file.	2017-08-04	not yet calculated	CVE-2017-12458 MISC
gnu_binutils -- gnu_binutils	The bfd_mach_o_read_symtab_strtab function in bfd/mach-o.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap write and possibly achieve code execution via a crafted mach-o file.	2017-08-04	not yet calculated	CVE-2017-12459 MISC
gnu_binutils -- gnu_binutils	The evax_bfd_print_emh function in vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file.	2017-08-04	not yet calculated	CVE-2017-12455 MISC
gnu_binutils -- gnu_binutils	The _bfd_vms_slurp_egsd function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an	2017-08-04	not yet calculated	CVE-2017-12454 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary memory read via a crafted vms alpha file.			
gnu_binutils -- gnu_binutils	The _bfd_xcoff_read_ar_hdr function in bfd/coff-rs6000.c and bfd/coff64-rs6000.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds stack read via a crafted COFF image file.	2017-08-04	not yet calculated	CVE-2017-12451 MISC
gnu_binutils -- gnu_binutils	The _bfd_vms_slurp_eeom function in libbfd.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file.	2017-08-04	not yet calculated	CVE-2017-12453 MISC
gnu_binutils -- gnu_binutils	The alpha_vms_object_p function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap write and possibly achieve code execution via a crafted vms alpha file.	2017-08-04	not yet calculated	CVE-2017-12450 MISC
gnu_binutils -- gnu_binutils	The _bfd_vms_save_sized_string function in vms-misc.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms file.	2017-08-04	not yet calculated	CVE-2017-12449 MISC
gnu_binutils -- gnu_binutils	The bfd_cache_close function in bfd/cache.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause a heap use after free and possibly achieve code execution via a crafted nested archive file. This issue occurs because incorrect functions are called during an attempt to release memory. The issue can be addressed by better input validation in the	2017-08-04	not yet calculated	CVE-2017-12448 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bfd_generic_archive_p function in bfd/archive.c.			
hashicorp -- vagrant_vmware_fusion_plugin	The sudo helper in the HashiCorp Vagrant VMware Fusion plugin (aka vagrant-vmware-fusion) before 4.0.21 allows local users to gain root privileges by leveraging failure to verify the path to the encoded ruby script or scrub the PATH variable.	2017-08-02	not yet calculated	CVE-2017-7642 FULLDISC CONFIRM(link is external) MISC(link is external)
heinekingmedia -- stashcat_for_android	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android, through 0.0.80w for Web, and through 0.0.86 for Desktop. For authentication, the user password is hashed directly with SHA-512 without a salt or another key-derivation mechanism to enable a secure secret for authentication. Moreover, only the first 32 bytes of the hash are used. This allows for easy dictionary and rainbow-table attacks if an attacker has access to the password hash.	2017-08-01	not yet calculated	CVE-2017-11131 MISC
heinekingmedia -- stashcat_for_android	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android, through 0.0.80w for Web, and through 0.0.86 for Desktop. The logout mechanism does not check for authorization. Therefore, an attacker only needs to know the device ID. This causes a denial of service. This might be interpreted as a vulnerability in customer-controlled software, in the sense that the StashCat client side has no secure way to signal that it is ending a session and that data should be deleted.	2017-08-01	not yet calculated	CVE-2017-11135 MISC
heinekingmedia -- stashcat_for_android	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android, through 0.0.80w for Web, and through 0.0.86 for Desktop. It uses RSA to exchange a secret for symmetric encryption of messages. However, the private RSA key is not only stored on the client but transmitted to the backend, too.	2017-08-01	not yet calculated	CVE-2017-11136 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Moreover, the key to decrypt the private key is composed of the first 32 bytes of the SHA-512 hash of the user password. But this hash is stored on the backend, too. Therefore, everyone with access to the backend database can read the transmitted secret for symmetric encryption, hence can read the communication.			
heinekingmedia -- stashcat_for_android	An issue was discovered in heinekingmedia StashCat before 1.5.18 for Android. No certificate pinning is implemented; therefore the attacker could issue a certificate for the backend and the application would not notice it.	2017-08-01	not yet calculated	CVE-2017-11132 MISC
heinekingmedia -- stashcat_for_android	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android, through 0.0.80w for Web, and through 0.0.86 for Desktop. To encrypt messages, AES in CBC mode is used with a pseudo-random secret. This secret and the IV are generated with math.random() in previous versions and with CryptoJS.lib.WordArray.random() in newer versions, which uses math.random() internally. This is not cryptographically strong.	2017-08-01	not yet calculated	CVE-2017-11133 MISC
heinekingmedia -- stashcat_for_android	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android, through 0.0.80w for Web, and through 0.0.86 for Desktop. The product's protocol only tries to ensure confidentiality. In the whole protocol, no integrity or authenticity checks are done. Therefore man-in-the-middle attackers can conduct replay attacks.	2017-08-01	not yet calculated	CVE-2017-11130 MISC
heinekingmedia -- stashcat_for_android	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android. The login credentials are written into a log file on the device. Hence, an attacker with access to the logs can read them.	2017-08-01	not yet calculated	CVE-2017-11134 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
heinekingmedia -- stashcat_for_android	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android. The keystore is locked with a hard-coded password. Therefore, everyone with access to the keystore can read the content out, for example the private key of the user.	2017-08-01	not yet calculated	CVE-2017-11129 MISC
hp -- linux_imaging_and_printing	The hp-plugin utility in HP Linux Imaging and Printing (HPLIP) makes it easier for man-in-the-middle attackers to execute arbitrary code by leveraging use of a short GPG key id from a keyserver to verify print plugin downloads.	2017-08-02	not yet calculated	CVE-2015-0839 FEDORA FEDORA MLIST(link is external) BID(link is external) UBUNTU(link is external) CONFIRM(link is external) CONFIRM(link is external)
i-o_data_device -- wn-ax1167gr_firmware	WN-AX1167GR firmware version 3.00 and earlier uses hardcoded credentials which may allow an attacker that can access the device to execute arbitrary code on the device.	2017-08-02	not yet calculated	CVE-2017-2280 MISC(link is external) JVN(link is external)
i-o_data_device -- wn-ax1167gr_firmware	WN-AX1167GR firmware version 3.00 and earlier allows an attacker to execute arbitrary OS commands via unspecified vectors.	2017-08-02	not yet calculated	CVE-2017-2281 MISC(link is external) JVN(link is external)
i-o_data_device -- wn-ax1167gr_firmware	Buffer overflow in WN-AX1167GR firmware version 3.00 and earlier allows an attacker to execute arbitrary commands via unspecified vectors.	2017-08-02	not yet calculated	CVE-2017-2282 MISC(link is external) JVN(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
i-o_data_device -- wn-g300r3_firmware	WN-G300R3 firmware version 1.0.2 and earlier uses hardcoded credentials which may allow an attacker that can access the device to execute arbitrary code on the device.	2017-08-02	not yet calculated	CVE-2017-2283 MISC(link is external) JVN(link is external)
ibm -- appscan_enterprise_edition	IBM AppScan Enterprise Edition 9.0 contains an unspecified vulnerability that could allow an attacker to hijack a valid user's session. IBM X-Force ID: 120257	2017-08-02	not yet calculated	CVE-2016-9981 CONFIRM(link is external) SECTRACK(link is external) MISC(link is external)
ibm -- content_navigator	IBM Content Navigator 2.0.3 and 3.0.0 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: 126233.	2017-08-04	not yet calculated	CVE-2017-1331 CONFIRM(link is external) BID(link is external) MISC(link is external)
ibm -- curam_social_program_management	IBM Curam Social Program Management 6.0 SP2 before EP26, 6.0.4 before 6.0.4.5iFix10 and 6.0.5 before 6.0.5.6 allows remote authenticated users to load arbitrary Java classes via unspecified vectors.	2017-08-02	not yet calculated	CVE-2014-8903 CONFIRM(link is external) BID(link is external)
ibm -- sterling_software	XML External Entity (XXE) vulnerability in IBM Sterling B2B Integrator 5.1 and 5.2 and IBM Sterling File Gateway 2.1 and 2.2 allows remote attackers to read arbitrary files via a crafted XML data.	2017-08-02	not yet calculated	CVE-2015-0194 AIXAPAR(link is external) CONFIRM(link is external) BID(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.6-2, a memory leak vulnerability was found in the function ReadMVGImage in coders/mvg.c, which allows attackers to cause a denial of	2017-08-05	not yet calculated	CVE-2017-12566 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	service, related to the function ReadSVGImage in svg.c.			
imagemagick -- imagemagick	In ImageMagick 7.0.6-2, a memory leak vulnerability was found in the function ReadOneJNGImage in coders/png.c, which allows attackers to cause a denial of service.	2017-08-05	not yet calculated	CVE-2017-12565 CONFIRM(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.6-2, a memory exhaustion vulnerability was found in the function ReadPSDImage in coders/psd.c, which allows attackers to cause a denial of service.	2017-08-05	not yet calculated	CVE-2017-12563 CONFIRM(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.6-2, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service.	2017-08-05	not yet calculated	CVE-2017-12564 CONFIRM(link is external)
intercom -- malion	MaLion for Windows and Mac versions 3.2.1 to 5.2.1 uses a hardcoded cryptographic key which may allow an attacker to alter the connection settings of Terminal Agent and spoof the Relay Service.	2017-08-04	not yet calculated	CVE-2017-10818 MISC(link is external) MISC(link is external)
intercom -- malion	MaLion for Mac 4.3.0 to 5.2.1 does not properly validate certificates, which may allow an attacker to eavesdrop on an encrypted communication.	2017-08-04	not yet calculated	CVE-2017-10819 MISC(link is external) MISC(link is external)
intercom -- malion	SQL injection vulnerability in the MaLion for Windows and Mac 5.0.0 to 5.2.1 allows remote attackers to execute arbitrary SQL commands via Relay Service Server.	2017-08-04	not yet calculated	CVE-2017-10816 MISC(link is external) MISC(link is external)
intercom -- malion	MaLion for Windows and Mac 5.0.0 to 5.2.1 allows remote attackers to bypass authentication to alter settings in Relay Service Server.	2017-08-04	not yet calculated	CVE-2017-10817 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC(link is external)
intercom -- malion	MaLion for Windows 5.2.1 and earlier (only when "Remote Control" is installed) and MaLion for Mac 4.0.1 to 5.2.1 (only when "Remote Control" is installed) allows remote attackers to bypass authentication to executue arbitrary commands or operations on Terminal Agent.	2017-08-04	not yet calculated	CVE-2017-10815 MISC(link is external) MISC(link is external)
internetsoft -- ftp_commander	InternetSoft FTP Commander 8.02 and prior has an untrusted search path, allowing DLL hijacking via a Trojan horse dwmapi.dll file.	2017-07-30	not yet calculated	CVE-2017-11749 MISC(link is external)
ioquake3 -- ioquake3	Buffer overflow in ioquake3 before 2017-08-02 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted packet.	2017-08-03	not yet calculated	CVE-2017-11721 MISC(link is external)
ip_messenger -- ip_messenger	Untrusted search path vulnerability in Installer of IP Messenger for Win 4.60 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-08-04	not yet calculated	CVE-2017-10820 MISC JVN(link is external)
jasper -- jasper	Double free vulnerability in the jasper_image_stop_load function in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via a crafted JPEG 2000 image file.	2017-08-02	not yet calculated	CVE-2015-5203 SUSE SUSE SUSE MLIST(link is external) REDHAT(link is external) CONFIRM(link is external) FEDORA FEDORA FEDORA GENTOO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ledger -- ledger	The ledger::parse_date_mask_routine function in times.cc in Ledger 3.1.1 allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted file.	2017-08-04	not yet calculated	CVE-2017-12482 MISC
ledger -- ledger	The find_option function in option.cc in Ledger 3.1.1 allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted file.	2017-08-04	not yet calculated	CVE-2017-12481 MISC
lenovo -- sierra_wireless_windows_mobile_ broadband_driver_packages	Multiple unquoted Windows search path vulnerabilities in Sierra Wireless Windows Mobile Broadband Driver Packages (MBDP) allow local users to gain privileges via a Trojan horse executable file.	2017-08-02	not yet calculated	CVE-2017-9247 CONFIRM(link is external) CONFIRM(link is external)
libgd -- libgd	The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.31 and 7.x before 7.1.7, does not zero colorMap arrays before use. A specially crafted GIF image could use the uninitialized tables to read ~700 bytes from the top of the stack, potentially disclosing sensitive information.	2017-08-02	not yet calculated	CVE-2017-7890 CONFIRM(link is external) CONFIRM(link is external) BID(link is external) CONFIRM(link is external) CONFIRM(link is external)
libmad -- libmad	The mad_decoder_run function in decoder.c in libmad 0.15.1b allows remote attackers to cause a denial of service (memory corruption) via a crafted MP3 file.	2017-08-01	not yet calculated	CVE-2017-11552 MISC
libsndfile -- libsndfile	Heap-based Buffer Overflow in the psf_binheader_writef function in common.c in libsndfile through 1.0.28 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.	2017-08-05	not yet calculated	CVE-2017-12562 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	Race condition in the fsnotify implementation in the Linux kernel through 4.12.4 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that leverages simultaneous execution of the inotify_handle_event and vfs_rename functions, as exploited in the wild in August 2017.	2017-08-05	not yet calculated	CVE-2017-7533 MISC MISC(link is external) BID(link is external) SECTRACK(link is external) MISC(link is external) MISC(link is external) MISC MISC MISC
manageengine -- desktop_central_9	Manage Engine Desktop Central 9 before build 90135 allows remote attackers to change passwords of users with the Administrator role via an addOrModifyUser operation to servlets/DCOperationsServlet.	2017-08-02	not yet calculated	CVE-2015-2560 MISC(link is external) BUGTRAQ(link is external) BID(link is external) CONFIRM(link is external)
manageengine -- opmanager	Zoho ManageEngine OpManager 11 through 12.2 uses a custom encryption algorithm to protect the credential used to access the monitored devices. The implemented algorithm doesn't use a per-system key or even a salt; therefore, it's possible to create a universal decryptor.	2017-08-03	not yet calculated	CVE-2015-9107 MISC(link is external)
mantisbt -- mantisbt	If, after successful installation of MantisBT through 2.5.2 on MySQL/MariaDB, the administrator does not remove the 'admin' directory (as recommended in the "Post-installation and upgrade tasks" section of the MantisBT Admin Guide), and the MySQL client has a local_infile setting enabled (in php.ini mysqli.allow_local_infile, or the MySQL	2017-08-05	not yet calculated	CVE-2017-12419 CONFIRM(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	client config file, depending on the PHP setup), an attacker may take advantage of MySQL's "connect file read" feature to remotely access files on the MantisBT server.			
mantisbt -- mantisbt	An XSS issue was discovered in admin/install.php in MantisBT before 1.3.12 and 2.x before 2.5.2. Some variables under user control in the MantisBT installation script are not properly sanitized before being output, allowing remote attackers to inject arbitrary JavaScript code, as demonstrated by the $f_database, $f_db_username, and $f_admin_username variables. This is mitigated by the fact that the admin/ folder should be deleted after installation, and also prevented by CSP.	2017-08-01	not yet calculated	CVE-2017-12061 CONFIRM(link is external) CONFIRM(link is external) SECTRACK(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM
mantisbt -- mantisbt	The "Project Documentation" feature in MantisBT 1.2.19 and earlier, when the threshold to access files ($g_view_proj_doc_threshold) is set to ANYBODY, allows remote authenticated users to download attachments linked to arbitrary private projects via a file id number in the file_id parameter to file_download.php.	2017-08-01	not yet calculated	CVE-2015-5059 FEDORA MLIST(link is external) MLIST(link is external) BID(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)
mantisbt -- mantisbt	An XSS issue was discovered in manage_user_page.php in MantisBT 2.x before 2.5.2. The 'filter' field is not sanitized before being rendered in the Manage User page, allowing remote attackers to execute arbitrary JavaScript code if CSP is disabled.	2017-08-01	not yet calculated	CVE-2017-12062 CONFIRM(link is external) CONFIRM(link is external) SECTRACK(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM(link is external) CONFIRM
mirth_corporation -- medhost_connex	MEDHOST Connex contains a hard-coded Mirth Connect admin credential that is used for customer Mirth Connect management access. An attacker with knowledge of the hard-coded credential and the ability to communicate directly with the Mirth Connect management console may be able to intercept sensitive patient information. The admin account password is hard-coded as $K8t1ng throughout the application, and is the same across all installations. Customers do not have the option to change the Mirth Connect admin account password. The Mirth Connect admin account is created during the Connex install. The plaintext account password is hard-coded multiple times in the Connex install and update scripts.	2017-07-31	not yet calculated	CVE-2017-11743 MISC BID(link is external)
nitro_software -- nitro_pro	Nitro Pro 11.0.3.173 allows remote attackers to execute arbitrary code via saveAs and launchURL calls with directory traversal sequences.	2017-08-03	not yet calculated	CVE-2017-7442 MISC(link is external) EXPLOIT-DB(link is external)
nosefart -- nosefart	The chk_mem_access function in cpu/nes6502/nes6502.c in libnosefart.a in Nosefart 2.9-mls allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted nsf file.	2017-07-31	not yet calculated	CVE-2017-11119 MISC
oneplus -- oneplus_2_primary_bootloader	The OnePlus 2 Primary Bootloader (PBL) does not validate the SBL1 partition before executing it, although it contains a certificate. This allows attackers with write access to that partition to disable signature validation.	2017-08-03	not yet calculated	CVE-2017-11105 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
palo_alto -- pan_os	The DNS Proxy in Palo Alto Networks PAN-OS before 6.1.18, 7.x before 7.0.16, 7.1.x before 7.1.11, and 8.x before 8.0.3 allows remote attackers to execute arbitrary code via a crafted domain name.	2017-08-02	not yet calculated	CVE-2017-8390 BID(link is external) SECTRACK(link is external) CONFIRM(link is external)
pervasive_software -- actian_psql_and_zen	Heap-based buffer overflow in Actian Pervasive PSQL v12.10 and Zen v13 allows remote attackers to execute arbitrary code via crafted traffic to TCP port 1583. The overflow occurs after Server-Client encryption-key exchange. The issue results from an integer underflow that leads to a zero-byte allocation. The _srvLnaConnectMP1 function is affected.	2017-07-31	not yet calculated	CVE-2017-11757 MISC(link is external) MISC(link is external) MISC(link is external)
potrace -- potrace	Potrace 1.14 has a heap-based buffer over-read in the interpolate_cubic function in mkbitmap.c.	2017-08-01	not yet calculated	CVE-2017-12067 MISC(link is external)
projeqtor -- projeqtor	uploadImage.php in ProjeQtOr before 6.3.2 allows remote authenticated users to execute arbitrary PHP code by uploading a .php file composed of concatenated image data and script data, as demonstrated by uploading as an image within the description text area.	2017-07-31	not yet calculated	CVE-2017-11760 CONFIRM
razer -- synapse	A specially crafted IOCTL can be issued to the rzpnk.sys driver in Razer Synapse that can cause an out of bounds read operation to occur due to a field within the IOCTL data being used as a length.	2017-08-02	not yet calculated	CVE-2017-9770 MISC(link is external)
razer -- synapse	A specially crafted IOCTL can be issued to the rzpnk.sys driver in Razer Synapse 2.20.15.1104 that is forwarded to ZwOpenProcess allowing a handle to be opened to an arbitrary process.	2017-08-02	not yet calculated	CVE-2017-9769 MISC(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sangoma_technologies -- freepbx	Multiple cross-site scripting (XSS) vulnerabilities in views/add-license-form.php in the Digium Addons module (digiumaddoninstaller) before 2.11.0.7 for FreePBX allow remote attackers to inject arbitrary web script or HTML via the (1) add_license_key, (2) add_license_first_name, (3) add_license_last_name, (4) add_license_company, (5) add_license_address1, (6) add_license_address2, (7) add_license_city, (8) add_license_state, (9) add_license_post_code, (10) add_license_country, (11) add_license_phone, or (12) add_license_email parameter in an add-license-form page to admin/config.php.	2017-08-02	not yet calculated	CVE-2015-2690 CONFIRM MISC(link is external) BUGTRAQ(link is external) BID(link is external) MISC(link is external)
shadow -- shadow	In shadow before 4.5, the newusers tool could be made to manipulate internal data structures in ways unintended by the authors. Malformed input may lead to crashes (with a buffer overflow or other memory corruption) or other unspecified behaviors. This crosses a privilege boundary in, for example, certain web-hosting environments in which a Control Panel allows an unprivileged user account to create subaccounts.	2017-08-04	not yet calculated	CVE-2017-12424 CONFIRM CONFIRM(link is external) CONFIRM(link is external)
slims_8_akasia -- slims_8_akasia	SLiMS 8 Akasia through 8.3.1 has an arbitrary file reading issue because of directory traversal in the url parameter to admin/help.php. It can be exploited by remote authenticated librarian users.	2017-08-05	not yet calculated	CVE-2017-12586 CONFIRM(link is external)
slims_8_akasia -- slims_8_akasia	SLiMS 8 Akasia through 8.3.1 has SQL injection in admin/AJAX_lookup_handler.php (tableName and tableFields parameters), admin/AJAX_check_id.php, and admin/AJAX_vocabolary_control.php. It can be exploited by remote authenticated librarian users.	2017-08-05	not yet calculated	CVE-2017-12585 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
slims_8_akasia -- slims_8_akasia	There is no CSRF mitigation in SLiMS 8 Akasia through 8.3.1. Also, an entire user profile (including the password) can be updated without sending the current password. This allows remote attackers to trick a user into changing to an attacker-controlled password, a complete account takeover, via the passwd1 and passwd2 fields in an admin/modules/system/app_user.php changecurrent=true operation.	2017-08-05	not yet calculated	CVE-2017-12584 CONFIRM(link is external)
sma_solar_technology -- multiple_products	An issue was discovered in SMA Solar Technology products. An attacker can use Sunny Explorer or the SMAdata2+ network protocol to update the device firmware without ever having to authenticate. If an attacker is able to create a custom firmware version that is accepted by the inverter, the inverter is compromised completely. This allows the attacker to do nearly anything: for example, giving access to the local OS, creating a botnet, using the inverters as a stepping stone into companies, etc.	2017-08-05	not yet calculated	CVE-2017-9860 MISC(link is external)
sma_solar_technology -- multiple_products	An issue was discovered in SMA Solar Technology products. The SIP implementation does not properly use authentication with encryption: it is vulnerable to replay attacks, packet injection attacks, and man in the middle attacks. An attacker is able to successfully use SIP to communicate with the device from anywhere within the LAN. An attacker may use this to crash the device, stop it from communicating with the SMA servers, exploit known SIP vulnerabilities, or find sensitive information from the SIP communications. Furthermore, because the SIP communication channel is unencrypted, an attacker capable of understanding the protocol can eavesdrop on communications. For example, passwords can be extracted.	2017-08-05	not yet calculated	CVE-2017-9861 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sma_solar_technology -- multiple_products	An Incorrect Password Management issue was discovered in SMA Solar Technology products. Default passwords exist that are rarely changed. User passwords will almost always be default. Installer passwords are expected to be default or similar across installations installed by the same company (but are sometimes changed). Hidden user accounts have (at least in some cases, though more research is required to test this for all hidden user accounts) a fixed password for all devices; it can never be changed by a user. Other vulnerabilities exist that allow an attacker to get the passwords of these hidden user accounts.	2017-08-05	not yet calculated	CVE-2017-9852 MISC(link is external)
sma_solar_technology -- multiple_products	An issue was discovered in SMA Solar Technology products. The inverters make use of a weak hashing algorithm to encrypt the password for REGISTER requests. This hashing algorithm can be cracked relatively easily. An attacker will likely be able to crack the password using offline crackers. This cracked password can then be used to register at the SMA servers.	2017-08-05	not yet calculated	CVE-2017-9859 MISC(link is external)
sma_solar_technology -- multiple_products	An issue was discovered in SMA Solar Technology products. An attacker can change the plant time even when not authenticated in any way. This changes the system time, possibly affecting lockout policies and random-number generators based on timestamps, and makes timestamps for data analysis unreliable.	2017-08-05	not yet calculated	CVE-2017-9864 MISC(link is external)
sma_solar_technology -- multiple_products	An issue was discovered in SMA Solar Technology products. By sending crafted packets to an inverter and observing the response, active and inactive user accounts can be determined. This aids in further attacks (such as a brute force attack) as one now knows exactly which users exist and which do not.	2017-08-05	not yet calculated	CVE-2017-9858 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sma_solar_technology -- multiple_products	An issue was discovered in SMA Solar Technology products. A secondary authentication system is available for Installers called the Grid Guard system. This system uses predictable codes, and a single Grid Guard code can be used on any SMA inverter. Any such code, when combined with the installer account, allows changing very sensitive parameters.	2017-08-05	not yet calculated	CVE-2017-9855 MISC(link is external)
sma_solar_technology -- multiple_products	An issue was discovered in SMA Solar Technology products. All inverters have a very weak password policy for the user and installer password. No complexity requirements or length requirements are set. Also, strong passwords are impossible due to a maximum of 12 characters and a limited set of characters.	2017-08-05	not yet calculated	CVE-2017-9853 MISC(link is external)
sma_solar_technology -- multiple_products	An issue was discovered in SMA Solar Technology products. Sniffed passwords from SMAdata2+ communication can be decrypted very easily. The passwords are "encrypted" using a very simple encryption algorithm. This enables an attacker to find the plaintext passwords and authenticate to the device.	2017-08-05	not yet calculated	CVE-2017-9856 MISC(link is external)
sma_solar_technology -- sunny_explorer	An issue was discovered in SMA Solar Technology products. If a user simultaneously has Sunny Explorer running and visits a malicious host, cross-site request forgery can be used to change settings in the inverters (for example, issuing a POST request to change the user password). All Sunny Explorer settings available to the authenticated user are also available to the attacker. (In some cases, this also includes changing settings that the user has no access to.) This may result in complete compromise of the device.	2017-08-05	not yet calculated	CVE-2017-9863 MISC(link is external)
sma_solar_technology -- sunny_explorer	An issue was discovered in SMA Solar Technology products. By sending nonsense data or setting up a TELNET session to the	2017-08-05	not yet calculated	CVE-2017-9851 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	database port of Sunny Explorer, the application can be crashed.			
sma_solar_technology -- sunny_explorer	An issue was discovered in SMA Solar Technology products. When signed into Sunny Explorer with a wrong password, it is possible to create a debug report, disclosing information regarding the application and allowing the attacker to create and save a .txt file with contents to his liking. An attacker may use this for information disclosure, or to write a file to normally unavailable locations on the local system.	2017-08-05	not yet calculated	CVE-2017-9862 MISC(link is external)
sma_solar_technology -- sunny_explorer	An issue was discovered in SMA Solar Technology products. By sniffing for specific packets on the localhost, plaintext passwords can be obtained as they are typed into Sunny Explorer by the user. These passwords can then be used to compromise the overall device.	2017-08-05	not yet calculated	CVE-2017-9854 MISC(link is external)
sma_solar_technology -- sunny_explorer	An issue was discovered in SMA Solar Technology products. The SMAdata2+ communication protocol does not properly use authentication with encryption: it is vulnerable to man in the middle, packet injection, and replay attacks. Any setting change, authentication packet, scouting packet, etc. can be replayed, injected, or used for a man in the middle session. All functionalities available in Sunny Explorer can effectively be done from anywhere within the network as long as an attacker gets the packet setup correctly. This includes the authentication process for all (including hidden) access levels and the changing of settings in accordance with the gained access rights. Furthermore, because the SMAdata2+ communication channel is unencrypted, an attacker capable of understanding the protocol can eavesdrop on communications.	2017-08-05	not yet calculated	CVE-2017-9857 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
socusoft -- flash_slideshow_maker_professional	SocuSoft Flash Slideshow Maker Professional through v5.20, when the advanced configuration is used, has an xml_path HTTP parameter that trusts user-supplied input, in conjunction with an unsafe XML configuration file. This has resultant content forgery, cross site scripting, and unvalidated redirection issues.	2017-08-05	not yet calculated	CVE-2017-12439 MISC(link is external)
sol.connect -- iset-mpp_meter	SQL injection vulnerability in SOL.Connect ISET-mpp meter 1.2.4.2 and earlier allows remote attackers to execute arbitrary SQL commands via the user parameter in a login action.	2017-08-02	not yet calculated	CVE-2017-11494 BUGTRAQ(link is external) BID(link is external)
sony -- nfc_port_software	Untrusted search path vulnerability in NFC Port Software remover Ver.1.3.0.1 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-08-02	not yet calculated	CVE-2017-2287 JVN(link is external)
sony -- nfc_port_software	Untrusted search path vulnerability in NFC Port Software Version 5.5.0.6 and earlier (for RC-S310, RC-S320, RC-S330, RC-S370, RC-S380, RC-S380/S), NFC Port Software Version 5.3.6.7 and earlier (for RC-S320, RC-S310/J1C, RC-S310/ED4C), PC/SC Activator for Type B Ver.1.2.1.0 and earlier, SFCard Viewer 2 Ver.2.5.0.0 and earlier, NFC Net Installer Ver.1.1.0.0 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-08-02	not yet calculated	CVE-2017-2286 JVN(link is external)
splunk -- enterprise	Persistent Cross Site Scripting (XSS) exists in Splunk Enterprise 6.5.x before 6.5.2, 6.4.x before 6.4.6, and 6.3.x before 6.3.9 and Splunk Light before 6.5.2, with exploitation requiring administrative access, aka SPL-134104.	2017-08-05	not yet calculated	CVE-2017-12572 CONFIRM(link is external)
technicolor -- tc7337_routers	Persistent XSS through the SSID of nearby Wi-Fi devices on Technicolor TC7337 routers 08.89.17.20.00 allows an attacker	2017-08-03	not yet calculated	CVE-2017-11320 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to cause DNS Poisoning and steal credentials from the router.			
technicolor -- tc8717t_devices	The Time Warner firmware on Technicolor TC8717T devices sets the default Wi-Fi passphrase to a combination of the SSID and BSSID, which makes it easier for remote attackers to obtain network access by reading a beacon frame.	2017-07-30	not yet calculated	CVE-2017-9522 MISC(link is external)
trello -- trello_app	Cross-site scripting (XSS) vulnerability in the Trello app before 4.0.8 for iOS might allow remote attackers to inject arbitrary web script or HTML by uploading and attaching a crafted photo to a Card.	2017-08-02	not yet calculated	CVE-2017-9244 CONFIRM(link is external)
trend_micro -- deep_discovery_director	Backup archives were found to be encrypted with a static password across different installations, which suggest the same password may be used in all virtual appliance instances of Trend Micro Deep Discovery Director 1.1.	2017-08-01	not yet calculated	CVE-2017-11380 CONFIRM(link is external) MISC(link is external)
trend_micro -- deep_discovery_director	Configuration and database backup archives are not signed or validated in Trend Micro Deep Discovery Director 1.1.	2017-08-01	not yet calculated	CVE-2017-11379 CONFIRM(link is external) MISC(link is external)
trend_micro -- officescan	Proxy command injection vulnerability in Trend Micro OfficeScan 11 and XG (12) allows remote attackers to execute arbitrary code on vulnerable installations. The specific flaw can be exploited by parsing the T parameter within Proxy.php. Formerly ZDI-CAN-4544.	2017-08-03	not yet calculated	CVE-2017-11394 BID(link is external) MISC(link is external) MISC(link is external)
twibright_labs -- links	The put_chars function in html_r.c in Twibright Links 2.14 allows remote attackers to cause a denial of service (buffer over-read) via a crafted HTML file.	2017-07-31	not yet calculated	CVE-2017-11114 MISC
unit4_polska -- teta_web	Session fixation vulnerability in Unit4 Polska TETA Web (formerly TETA Galactica) 22.62.3.4 and earlier allows	2017-08-02	not yet calculated	CVE-2015-1174

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote attackers to hijack web sessions via a session id.			MISC(link is external)
varnish_cache_http -- varnish_cache_http	An issue was discovered in Varnish HTTP Cache 4.0.1 through 4.0.4, 4.1.0 through 4.1.7, 5.0.0, and 5.1.0 through 5.1.2. A wrong if statement in the varnishd source code means that particular invalid requests from the client can trigger an assert, related to an Integer Overflow. This causes the varnishd worker process to abort and restart, losing the cached contents in the process. An attacker can therefore crash the varnishd worker process on demand and effectively keep it from serving content - a Denial-of-Service attack. The specific source-code filename containing the incorrect statement varies across releases.	2017-08-04	not yet calculated	CVE-2017-12425 CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM CONFIRM
vit_software -- spider_player	VIT Spider Player 2.5.3 has an untrusted search path, allowing DLL hijacking via a Trojan horse dwmapi.dll, olepro32.dll, dsound.dll, or AUDIOSES.dll file.	2017-07-30	not yet calculated	CVE-2017-11748 MISC(link is external)
vmware -- vcenter_server	VMware vCenter Server 5.5, 6.0, 6.5 allows vSphere users with certain, limited vSphere privileges to use the VIX API to access Guest Operating Systems without the need to authenticate.	2017-07-28	not yet calculated	CVE-2017-4919 BID(link is external) SECTRACK(link is external) CONFIRM(link is external)
vmware -- vmware	VMware Tools prior to 10.0.9 contains multiple file system races in libDeployPkg, related to the use of hard-coded paths under /tmp. Successful exploitation of this issue may result in a local privilege escalation. CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H	2017-07-28	not yet calculated	CVE-2015-5191 BID(link is external) SECTRACK(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Event List plugin 0.7.9 for WordPress has XSS in the slug array parameter to wp-admin/admin.php in an el_admin_categories delete_bulk action.	2017-08-01	not yet calculated	CVE-2017-12068 MISC(link is external)
wordpress -- wordpress	The Etoile Ultimate Product Catalog plugin 4.2.11 for WordPress has XSS in the Add Product Manually component.	2017-08-02	not yet calculated	CVE-2017-12200 MISC(link is external)
wordpress -- wordpress	The Easy Testimonials plugin 3.0.4 for WordPress has XSS in include/settings/display.options.php, as demonstrated by the Default Testimonials Width, View More Testimonials Link, and Testimonial Excerpt Options screens.	2017-08-01	not yet calculated	CVE-2017-12131 MISC(link is external)
yaml-cpp -- yaml-cpp	The function "Token& Scanner::peek" in scanner.cpp in yaml-cpp 0.5.3 and earlier allows remote attackers to cause a denial of service (assertion failure and application exit) via a '!2' string.	2017-07-30	not yet calculated	CVE-2017-11692 MISC(link is external)
ztrela_knowledge_solutions -- eapmd5pass	A length validation (leading to out-of-bounds read and write) flaw was found in the way eapmd5pass 1.4 handled network traffic in the extract_eapusername function. A remote attacker could potentially use this flaw to crash the eapmd5pass process by generating specially crafted network traffic.	2017-07-31	not yet calculated	CVE-2017-11670 MISC(link is external)
ztrela_knowledge_solutions -- eapmd5pass	An out-of-bounds read flaw related to the assess_packet function in eapmd5pass.c:211 was found in the way eapmd5pass 1.4 handled processing of network packets. A remote attacker could potentially use this flaw to crash the eapmd5pass process under certain circumstances by generating specially crafted network traffic.	2017-07-31	not yet calculated	CVE-2017-11669 MISC(link is external)
ztrela_knowledge_solutions -- eapmd5pass	An out-of-bounds read flaw related to the assess_packet function in eapmd5pass.c:134 was found in the way eapmd5pass 1.4 handled processing of network packets. A remote attacker could	2017-07-31	not yet calculated	CVE-2017-11668 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	potentially use this flaw to crash the eapmd5pass process under certain circumstances by generating specially crafted network traffic.			