Vulnerability Summary for the Week of May 29, 2017

Please Note:

• The vulnerabilities are categorized by their level of severity which is either High, Medium or Low.

• The CVE identity number is the publicly known ID given to that particular vulnerability. Therefore, you can search the status of that particular vulnerability using that ID.

• The CVSS (Common Vulnerability Scoring System) score is a standard scoring system used to determine the severity of the vulnerability.

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
There were no high vulnerabilities recorded this week.				

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
apache -- hive	Apache Hive (JDBC + HiveServer2) implements SSL for plain TCP and HTTP connections (it supports both transport modes). While validating the server's certificate during the connection setup, the client in Apache Hive before 1.2.2 and 2.0.x before 2.0.1 doesn't seem to be verifying the common name attribute of the certificate. In this way, if a JDBC client sends an SSL request to server abc.com, and the server responds with a valid certificate (certified by CA) but issued to xyz.com, the client will accept that as a valid certificate and the SSL handshake will go through.	2017-05-30	5.0	CVE-2016-3083 BID(link is external) MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fortinet -- fortiportal	An improper Access Control vulnerability in Fortinet FortiPortal versions 4.0.0 and below allows an attacker to interact with unauthorized VDOMs or enumerate other ADOMs via another user's stolen session and CSRF tokens or the adomName parameter in the /fpc/sec/customer/policy/getAdomVersion request.	2017-05-26	6.4	CVE-2017-7337 CONFIRM(link is external)
fortinet -- fortiportal	A password management vulnerability in Fortinet FortiPortal versions 4.0.0 and below allows an attacker to carry out information disclosure via the FortiAnalyzer Management View.	2017-05-26	5.0	CVE-2017-7338 CONFIRM(link is external)
fortinet -- fortiportal	A Cross-Site Scripting vulnerability in Fortinet FortiPortal versions 4.0.0 and below allows an attacker to execute unauthorized code or commands via the 'Name' and 'Description' inputs in the 'Add Revision Backup' functionality.	2017-05-26	4.3	CVE-2017-7339 CONFIRM(link is external)
fortinet -- fortiportal	An open redirect vulnerability in Fortinet FortiPortal 4.0.0 and below allows attacker to execute unauthorized code or commands via the url parameter.	2017-05-26	5.8	CVE-2017-7343 CONFIRM(link is external)
fortinet -- fortiportal	A weak password recovery vulnerability in Fortinet FortiPortal versions 4.0.0 and below allows attacker to carry out information disclosure via the Forgotten Password feature.	2017-05-26	5.0	CVE-2017-7731 CONFIRM(link is external)
fortinet -- fortiweb	A Cross-Site Scripting vulnerability in Fortinet FortiWeb versions 5.7.1 and below allows attacker to execute unauthorized code or commands via an improperly sanitized POST	2017-05-26	4.3	CVE-2017-3129 BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameter in the FortiWeb Site Publisher feature.			CONFIRM(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: 125976.	2017-05-26	4.3	CVE-2017-1325 CONFIRM(link is external) MISC(link is external)
ibm -- maximo_asset_management_essentials	IBM Maximo Asset Management 7.5 and 7.6 generates error messages that could reveal sensitive information that could be used in further attacks against the system. IBM X-Force ID: 125153.	2017-05-26	5.0	CVE-2017-1292 CONFIRM(link is external) MISC(link is external)
linux -- linux_kernel	The __ip6_append_data function in net/ipv6/ip6_output.c in the Linux kernel through 4.11.3 is too late in checking whether an overwrite of an skb data structure may occur, which allows local users to cause a denial of service (system crash) via crafted system calls.	2017-05-26	4.9	CVE-2017-9242 CONFIRM BID(link is external) CONFIRM(link is external) CONFIRM

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- maximo_asset_management_essentials	IBM Maximo Asset Management 7.5 and 7.6 is vulnerable to HTTP response splitting attacks. A remote attacker could exploit this vulnerability using specially-crafted URL to cause the server to return a split response, once the URL is clicked. This would	2017-05-26	3.5	CVE-2017-1291 CONFIRM(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allow the attacker to perform further attacks, such as Web cache poisoning, cross-site scripting, and possibly obtain sensitive information. IBM X-Force ID: 125152.			

Severity Not Yet Assigned				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
allen_disk -- allen_disk	SSRF vulnerability in remotedownload.php in Allen Disk 1.6 allows remote authenticated users to conduct port scans and access intranet servers via a crafted file parameter.	2017-05-31	not yet calculated	CVE-2017-9307 MISC(link is external)
allen_disk -- allen_disk	Cross-site scripting (XSS) vulnerability in Allen Disk 1.6 allows remote authenticated users to inject arbitrary web script or HTML persistently by uploading a crafted HTML file. The attack vector is the content of this file, and the filename must be specified in the PATH_INFO to readfile.php.	2017-05-28	not yet calculated	CVE-2017-9249 BID(link is external) MISC(link is external)
andrzuk/finecms -- andrzuk/finecms	andrzuk/FineCMS through 2017-05-28 is vulnerable to a reflected XSS in the search page via the text-search parameter to index.php in a route=search action.	2017-05-28	not yet calculated	CVE-2017-9252 MISC(link is external)
andrzuk/finecms -- andrzuk/finecms	andrzuk/FineCMS through 2017-05-28 is vulnerable to a reflected XSS in the sitename parameter to admin.php.	2017-05-28	not yet calculated	CVE-2017-9251 MISC(link is external)
apache -- knox	For versions of Apache Knox from 0.2.0 to 0.11.0 - an authenticated user may use a specially crafted URL to impersonate another user while accessing WebHDFS through Apache Knox. This may result in escalated privileges and unauthorized data access. While this activity is audit logged and can be easily associated with the authenticated user, this is still a serious security issue. All users are recommended to upgrade to the Apache Knox 0.12.0 release.	2017-05-26	not yet calculated	CVE-2017-5646 MLIST BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- open_vswitch	In Open vSwitch (OvS) v2.7.0, there is a buffer over-read while parsing the group mod OpenFlow message sent from the controller in `lib/ofp-util.c` in the function `ofputil_pull_ofp15_group_mod`.	2017-05-29	not yet calculated	CVE-2017-9265 CONFIRM
apache -- open_vswitch	In Open vSwitch (OvS) 2.5.0, a malformed IP packet can cause the switch to read past the end of the packet buffer due to an unsigned integer underflow in `lib/flow.c` in the function `miniflow_extract`, permitting remote bypass of the access control list enforced by the switch.	2017-05-29	not yet calculated	CVE-2016-10377 CONFIRM
apache -- open_vswitch	In Open vSwitch (OvS) 2.7.0, while parsing an OpenFlow role status message, there is a call to the abort() function for undefined role status reasons in the function `ofp_print_role_status_message` in `lib/ofp-print.c` that may be leveraged toward a remote DoS attack by a malicious switch.	2017-05-29	not yet calculated	CVE-2017-9263 CONFIRM
apache -- open_vswitch	In lib/conntrack.c in the firewall implementation in Open vSwitch (OvS) 2.6.1, there is a buffer over-read while parsing malformed TCP, UDP, and IPv6 packets in the functions `extract_l3_ipv6`, `extract_l4_tcp`, and `extract_l4_udp` that can be triggered remotely.	2017-05-29	not yet calculated	CVE-2017-9264 CONFIRM
aries -- qwr-1104_wireless-n_router	Aries QWR-1104 Wireless-N Router with Firmware Version WRC.253.2.0913 has XSS on the Wireless Site Survey page, exploitable with the name of an access point.	2017-05-28	not yet calculated	CVE-2017-9243 MISC(link is external) EXPLOIT-DB(link is external)
atlassian -- eucalyptus	Atlassian Eucalyptus before 4.4.1, when in EDGE mode, allows remote authenticated users with certain privileges to cause a denial of service (E2 service outage) via unspecified vectors.	2017-06-01	not yet calculated	CVE-2017-7999 CONFIRM(link is external)
bigtree -- bigtree	Unrestricted File Upload exists in BigTree CMS through 4.2.18: if an attacker uploads an 'xxx.pht' or 'xxx.phtml' file, they could bypass a safety check and execute any code.	2017-06-02	not yet calculated	CVE-2017-9364 CONFIRM(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				external) CONFIRM(link is external)
bigtree -- bigtree	CSRF exists in BigTree CMS through 4.2.18 with the force parameter to /admin/pages/revisions.php - for example: /admin/pages/revisions/1/?force=false. A page with id=1 can be unlocked.	2017-06-02	not yet calculated	CVE-2017-9365 CONFIRM(link is external) CONFIRM(link is external)
bigtree -- bigtree	BigTree CMS through 4.2.18 does not prevent a user from deleting their own account. This could have security relevance because deletion was supposed to be an admin-only action, and the admin may have other tasks (such as data backups) to complete before a user is deleted.	2017-06-02	not yet calculated	CVE-2017-9378 MISC(link is external) MISC(link is external)
bigtree -- bigtree	Multiple CSRF issues exist in BigTree CMS through 4.2.18 - the clear parameter to core\admin\modules\dashboard\vitals-statistics\404\clear.php and the from or to parameter to core\admin\modules\dashboard\vitals-statistics\404\create-301.php.	2017-06-02	not yet calculated	CVE-2017-9379 MISC(link is external)
bram_korsten_note -- bram_korsten_note	Bram Korsten Note through 1.2.0 is vulnerable to a reflected XSS in note-source\ui\editor.php (edit parameter).	2017-05-29	not yet calculated	CVE-2017-9289 CONFIRM(link is external)
canonical -- juju	Juju before 1.25.12, 2.0.x before 2.0.4, and 2.1.x before 2.1.3 uses a UNIX domain socket without setting appropriate permissions, allowing privilege escalation by users on the system to root.	2017-05-27	not yet calculated	CVE-2017-9232 BID(link is external) CONFIRM(link is external)
ceragon -- fibeair_ip-10	Ceragon FibeAir IP-10 have a default SSH public key in the authorized_keys file for the mateidu user, which allows remote attackers to	2017-06-01	not yet calculated	CVE-2015-0936 MISC(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	obtain SSH access by leveraging knowledge of the private key.			external) MISC(link is external) FULLDISC BID(link is external) MISC(link is external) MISC(link is external)
chicken_scheme -- chicken_scheme	An incorrect "pair?" check in the Scheme "length" procedure results in an unsafe pointer dereference in all CHICKEN Scheme versions prior to 4.13, which allows an attacker to cause a denial of service by passing an improper list to an application that calls "length" on it.	2017-06-01	not yet calculated	CVE-2017-9334 CONFIRM CONFIRM
cygnux.org -- syspass	inc/SP/Html/Html.class.php in sysPass 2.1.9 allows remote attackers to bypass the XSS filter, as demonstrated by use of an "<svg/onload=" substring instead of an "<svg onload=" substring.	2017-05-31	not yet calculated	CVE-2017-9306 MISC(link is external)
digium -- asterisk	The multi-part body parser in PJSIP, as used in Asterisk Open Source 13.x before 13.15.1 and 14.x before 14.4.1, Certified Asterisk 13.13 before 13.13-cert4, and other products, allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet.	2017-06-02	not yet calculated	CVE-2017-9359 CONFIRM CONFIRM CONFIRM
digium -- asterisk	A memory exhaustion vulnerability exists in Asterisk Open Source 13.x before 13.15.1 and 14.x before 14.4.1 and Certified Asterisk 13.13 before 13.13-cert4, which can be triggered by sending specially crafted SCCP packets causing a infinite loop and leading to memory exhaustion (by message logging in that loop).	2017-06-02	not yet calculated	CVE-2017-9358 CONFIRM CONFIRM
digium -- asterisk	PJSIP, as used in Asterisk Open Source 13.x before 13.15.1 and 14.x before 14.4.1, Certified Asterisk 13.13 before 13.13-cert4, and other products, allows remote attackers to cause a denial of service (buffer overflow and application crash) via a SIP packet with a crafted	2017-06-02	not yet calculated	CVE-2017-9372 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CSeq header in conjunction with a Via header that lacks a branch parameter.			
e107 -- e107	e107 2.1.1 allows SQL injection by remote authenticated administrators via the pagelist parameter to e107_admin/menus.php, related to the menuSaveVisibility function.	2017-05-29	not yet calculated	CVE-2016-10378 MISC(link is external)
exiv2 -- exiv2	An issue was discovered in Exiv2 0.26. When the data structure of the structure ifd is incorrect, the program assigns pValue_ to 0x0, and the value of pValue() is 0x0. TiffImageEntry::doWriteImage will use the value of pValue() to cause a segmentation fault. To exploit this vulnerability, someone must open a crafted tiff file.	2017-05-26	not yet calculated	CVE-2017-9239 MISC BID(link is external) MISC(link is external)
flipbuilder -- flipbuilder	Cross-site scripting (XSS) vulnerability in FlipBuilder Flip PDF allows remote attackers to inject arbitrary web script or HTML via the currentHTMLURL parameter.	2017-06-01	not yet calculated	CVE-2017-7384 MISC(link is external)
forinet -- fortiwlc-sd	An escalation of privilege vulnerability in Fortinet FortiWLC-SD versions 8.2.4 and below allows attacker to gain root access via the CLI command 'copy running-config'.	2017-05-26	not yet calculated	CVE-2017-3134 BID(link is external) CONFIRM(link is external)
fortinet -- forticlient	A potential execution of unauthorized code or commands vulnerability in Fortinet FortiClient SSL_VPN Linux versions available with FortiOS 5.4.2 and below allows attacker to potentially overwrite an existing file via the FortiClient log file.	2017-05-26	not yet calculated	CVE-2016-8496 BID(link is external) CONFIRM(link is external)
fortinet -- forticlient	An escalation of privilege vulnerability in Fortinet FortiClient SSL_VPN Linux versions available with FortiOS 5.4.3 and below allows an attacker to gain root privilege via the subproc file.	2017-05-26	not yet calculated	CVE-2016-8497 BID(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fortinet -- fortigate	A Cross-Site Scripting vulnerability in Fortinet FortiGate 5.2.0 through 5.2.10 allows attacker to execute unauthorized code or commands via the srcintf parameter during Firewall Policy Creation.	2017-06-01	not yet calculated	CVE-2017-3127 BID(link is external) CONFIRM(link is external)
fortinet -- fortinet_fortianalyzer	An Open Redirect vulnerability in Fortinet FortiAnalyzer 5.4.0 through 5.4.2 and FortiManager 5.4.0 through 5.4.2 allows attacker to execute unauthorized code or commands via the next parameter.	2017-05-26	not yet calculated	CVE-2017-3126 BID(link is external) CONFIRM(link is external)
freeradius -- freeradius	The TLS session cache in FreeRADIUS before 3.0.14 fails to reliably prevent resumption of an unauthenticated session, which allows remote attackers (such as malicious 802.1X supplicants) to bypass authentication via PEAP or TTLS.	2017-05-29	not yet calculated	CVE-2017-9148 MISC MISC BID(link is external)
git -- git-shell	git-shell in git before 2.4.12, 2.5.x before 2.5.6, 2.6.x before 2.6.7, 2.7.x before 2.7.5, 2.8.x before 2.8.5, 2.9.x before 2.9.4, 2.10.x before 2.10.3, 2.11.x before 2.11.2, and 2.12.x before 2.12.3 might allow remote authenticated users to gain privileges via a repository name that starts with a - (dash) character.	2017-06-01	not yet calculated	CVE-2017-8386 SUSE MLIST DEBIAN BID(link is external) SECTRACK (link is external) UBUNTU(link is external) MISC(link is external) CONFIRM(link is external) FEDORA FEDORA FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hitachi -- device_manager	XXE vulnerability in Hitachi Device Manager before 8.5.2-01 and Hitachi Replication Manager before 8.5.2-00 allows authenticated remote users to read arbitrary files.	2017-05-29	not yet calculated	CVE-2017-9295 CONFIRM(link is external) BID(link is external)
hitachi -- device_manager	Cross-site scripting vulnerability in Hitachi Device Manager before 8.5.2-01 and Hitachi Replication Manager before 8.5.2-00 allows authenticated remote users to execute arbitrary JavaScript code.	2017-05-29	not yet calculated	CVE-2017-9298 CONFIRM(link is external)
hitachi -- device_manager	Open Redirect vulnerability in Hitachi Device Manager before 8.5.2-01 allows remote attackers to redirect users to arbitrary web sites.	2017-05-29	not yet calculated	CVE-2017-9297 CONFIRM(link is external) BID(link is external)
hitachi -- device_manager	Open Redirect vulnerability in Hitachi Device Manager before 8.5.2-01 and Hitachi Tuning Manager before 8.5.2-00 allows remote attackers to redirect authenticated users to arbitrary web sites.	2017-05-29	not yet calculated	CVE-2017-9296 CONFIRM(link is external) BID(link is external)
hitachi -- device_manager	RMI vulnerability in Hitachi Device Manager before 8.5.2-01 allows remote attackers to execute internal commands without authentication via RMI ports.	2017-05-29	not yet calculated	CVE-2017-9294 CONFIRM(link is external) BID(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.5-5, the ReadMPCImage function in mpc.c allows attackers to cause a denial of service (memory leak) via a crafted file.	2017-06-02	not yet calculated	CVE-2017-9409 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
imagemagick -- imagemagick	In ImageMagick 7.0.5-5, the ReadPALMImage function in palm.c allows attackers to cause a denial of service (memory leak) via a crafted file.	2017-06-02	not yet calculated	CVE-2017-9407 CONFIRM(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.5-5, the ReadICONImage function in icon.c:452 allows attackers to cause a denial of service (memory leak) via a crafted file.	2017-06-02	not yet calculated	CVE-2017-9405 CONFIRM(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.5-6 Q16, the ReadJNGImage function in coders/png.c allows attackers to cause a denial of service (memory leak) via a crafted file.	2017-05-29	not yet calculated	CVE-2017-9262 BID(link is external) CONFIRM(link is external)
imagemagick -- imagemagick	In ImageMagick 7.0.5-6 Q16, the ReadMNGImage function in coders/png.c allows attackers to cause a denial of service (memory leak) via a crafted file.	2017-05-29	not yet calculated	CVE-2017-9261 BID(link is external) CONFIRM(link is external)
intel -- solid_state	There is an escalation of privilege vulnerability in the Intel Solid State Drive Toolbox versions before 3.4.5 which allow a local administrative attacker to load and execute arbitrary code.	2017-05-31	not yet calculated	CVE-2017-5688 BID(link is external) CONFIRM(link is external)
jerryscript -- jerryscript	The lexer_process_char_literal function in jerry-core/parser/js/js-lexer.c in JerryScript 1.0 does not skip memory allocation for empty strings, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via malformed JavaScript source code, related to the jmem_heap_free_block function.	2017-05-28	not yet calculated	CVE-2017-9250 CONFIRM(link is external) CONFIRM(link is external) CONFIRM(li

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				nk is external)
joomla -- joomla	The VirtueMart com_virtuemart component 3.0.14 for Joomla! allows SQL injection by remote authenticated administrators via the virtuemart_paymentmethod_id or virtuemart_shipmentmethod_id parameter to administrator/index.php.	2017-05-29	not yet calculated	CVE-2016-10379 MISC(link is external) BID(link is external)
juniper_networks -- junos_os	On Juniper Networks products or platforms running Junos OS 12.1X46 prior to 12.1X46-D55, 12.1X47 prior to 12.1X47-D45, 12.3R13 prior to 12.3R13, 12.3X48 prior to 12.3X48-D35, 13.3 prior to 13.3R10, 14.1 prior to 14.1R8, 14.1X53 prior to 14.1X53-D40, 14.1X55 prior to 14.1X55-D35, 14.2 prior to 14.2R6, 15.1 prior to 15.1F2 or 15.1R1, 15.1X49 prior to 15.1X49-D20 where the BGP add-path feature is enabled with 'send' option or with both 'send' and 'receive' options, a network based attacker can cause the Junos OS rpd daemon to crash and restart. Repeated crashes of the rpd daemon can result in an extended denial of service condition.	2017-05-30	not yet calculated	CVE-2017-2302 BID(link is external) CONFIRM(link is external)
juniper_networks -- junos_os	On Juniper Networks products or platforms running Junos OS 12.1X46 prior to 12.1X46-D50, 12.1X47 prior to 12.1X47-D40, 12.3 prior to 12.3R13, 12.3X48 prior to 12.3X48-D30, 13.2X51 prior to 13.2X51-D40, 13.3 prior to 13.3R10, 14.1 prior to 14.1R8, 14.1X53 prior to 14.1X53-D35, 14.1X55 prior to 14.1X55-D35, 14.2 prior to 14.2R5, 15.1 prior to 15.1F6 or 15.1R3, 15.1X49 prior to 15.1X49-D30 or 15.1X49-D40, 15.1X53 prior to 15.1X53-D35, and where RIP is enabled, certain RIP advertisements received by the router may cause the RPD daemon to crash resulting in a denial of service condition.	2017-05-30	not yet calculated	CVE-2017-2303 BID(link is external) CONFIRM(link is external)
juniper_networks -- junos_os	On Juniper Networks products or platforms running Junos OS 11.4 prior to 11.4R13-S3, 12.1X46 prior to 12.1X46-D60, 12.3 prior to 12.3R12-S2 or 12.3R13, 12.3X48 prior to 12.3X48-D40, 13.2X51 prior to 13.2X51-D40,	2017-05-30	not yet calculated	CVE-2017-2301 BID(link is external) CONFIRM(li

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	13.3 prior to 13.3R10, 14.1 prior to 14.1R8, 14.1X53 prior to 14.1X53-D12 or 14.1X53-D35, 14.1X55 prior to 14.1X55-D35, 14.2 prior to 14.2R7, 15.1 prior to 15.1F6 or 15.1R3, 15.1X49 prior to 15.1X49-D60, 15.1X53 prior to 15.1X53-D30 and DHCPv6 enabled, when a crafted DHCPv6 packet is received from a subscriber, jdhcpd daemon crashes and restarts. Repeated crashes of the jdhcpd process may constitute an extended denial of service condition for subscribers attempting to obtain IPv6 addresses.			nk is external)
juniper_networks -- junos_os	Juniper Networks QFX3500, QFX3600, QFX5100, QFX5200, EX4300 and EX4600 devices running Junos OS 14.1X53 prior to 14.1X53-D40, 15.1X53 prior to 15.1X53-D40, 15.1 prior to 15.1R2, do not pad Ethernet packets with zeros, and thus some packets can contain fragments of system memory or data from previous packets. This issue is also known as 'Etherleak'	2017-05-30	not yet calculated	CVE-2017-2304 BID(link is external) CONFIRM(link is external)
juniper_networks -- junos_space	On Juniper Networks Junos Space versions prior to 16.1R1, an unauthenticated remote attacker with network access to Junos space device can easily create a denial of service condition.	2017-05-30	not yet calculated	CVE-2017-2311 BID(link is external) CONFIRM(link is external)
juniper_networks -- junos_space	An XML External Entity Injection vulnerability in Juniper Networks Junos Space versions prior to 16.1R1 may allow an authenticated user to read arbitrary files on the device.	2017-05-30	not yet calculated	CVE-2017-2308 BID(link is external) CONFIRM(link is external)
juniper_networks -- junos_space	On Juniper Networks Junos Space versions prior to 16.1R1 when certificate based authentication is enabled for the Junos Space cluster, some restricted web services are accessible over the network. This represents an information leak risk.	2017-05-30	not yet calculated	CVE-2017-2309 BID(link is external) CONFIRM(li

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				nk is external)
juniper_networks -- junos_space	A firewall bypass vulnerability in the host based firewall of Juniper Networks Junos Space versions prior to 16.1R1 may permit certain crafted packets, representing a network integrity risk.	2017-05-30	not yet calculated	CVE-2017-2310 BID(link is external) CONFIRM(link is external)
juniper_networks -- junos_space	A reflected cross site scripting vulnerability in the administrative interface of Juniper Networks Junos Space versions prior to 16.1R1 may allow remote attackers to steal sensitive information or perform certain administrative actions on Junos Space.	2017-05-30	not yet calculated	CVE-2017-2307 BID(link is external) CONFIRM(link is external)
juniper_networks -- junos_space	On Juniper Networks Junos Space versions prior to 16.1R1, due to an insufficient authorization check, readonly users on the Junos Space administrative web interface can create privileged users, allowing privilege escalation.	2017-05-30	not yet calculated	CVE-2017-2305 BID(link is external) CONFIRM(link is external)
juniper_networks -- junos_space	On Juniper Networks Junos Space versions prior to 16.1R1, due to an insufficient authorization check, readonly users on the Junos Space administrative web interface can execute code on the device.	2017-05-30	not yet calculated	CVE-2017-2306 BID(link is external) CONFIRM(link is external)
juniper_networks -- srx_series_services_gateways	On Juniper Networks SRX Series Services Gateways chassis clusters running Junos OS 12.1X46 prior to 12.1X46-D65, 12.3X48 prior to 12.3X48-D40, 12.3X48 prior to 12.3X48-D60, flowd daemon on the primary node of an SRX Series chassis cluster may crash and restart when attempting to synchronize a multicast session created via crafted multicast packets.	2017-05-30	not yet calculated	CVE-2017-2300 BID(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lansweeper -- lansweeper	Lansweeper before 6.0.0.65 has XSS in an image retrieval URI, aka Bug 542782.	2017-05-29	not yet calculated	CVE-2017-9292 CONFIRM(link is external)
laravel -- laravel	Laravel 5.4.x before 5.4.22 does not properly constrain the host portion of a password-reset URL, which makes it easier for remote attackers to conduct phishing attacks by specifying an attacker-controlled host.	2017-05-29	not yet calculated	CVE-2017-9303 BID(link is external) CONFIRM(link is external)
libming -- libming	The readString function in util/read.c and util/old/read.c in libming 0.4.8 allows remote attackers to cause a denial of service via a large file that is mishandled by listswf, listaction, etc. This occurs because of an integer overflow that leads to a memory allocation error.	2017-05-31	not yet calculated	CVE-2017-8782 MISC
libtiff -- libtiff	In LibTIFF 4.0.7, a memory leak vulnerability was found in the function TIFFReadDirEntryLong8Array in tif_dirread.c, which allows attackers to cause a denial of service via a crafted file.	2017-06-02	not yet calculated	CVE-2017-9403 CONFIRM
libtiff -- libtiff	In LibTIFF 4.0.7, a memory leak vulnerability was found in the function OJPEGReadHeaderInfoSecTablesQTable in tif_ojpeg.c, which allows attackers to cause a denial of service via a crafted file.	2017-06-02	not yet calculated	CVE-2017-9404 CONFIRM
microsoft -- malware_protection_engine	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka "Microsoft Malware Protection Engine Denial of Service Vulnerability", a different vulnerability than	2017-05-26	not yet calculated	CVE-2017-8537 BID(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVE-2017-8535, CVE-2017-8536, CVE-2017-8539, and CVE-2017-8542.			
microsoft -- malware_protection_engine	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to memory corruption. aka "Microsoft Malware Protection Engine Remote Code Execution Vulnerability", a different vulnerability than CVE-2017-8540 and CVE-2017-8541.	2017-05-26	not yet calculated	CVE-2017-8538 BID(link is external) CONFIRM(link is external)
microsoft -- malware_protection_engine	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to memory corruption. aka "Microsoft Malware Protection Engine Remote Code Execution Vulnerability", a different vulnerability than CVE-2017-8538 and CVE-2017-8541.	2017-05-26	not yet calculated	CVE-2017-8540 BID(link is external) CONFIRM(link is external)
microsoft -- malware_protection_engine	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to memory corruption. aka "Microsoft Malware Protection Engine Remote Code Execution Vulnerability", a different vulnerability than CVE-2017-8538 and CVE-2017-8540.	2017-05-26	not yet calculated	CVE-2017-8541 BID(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- malware_protection_engine	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka "Microsoft Malware Protection Engine Denial of Service Vulnerability", a different vulnerability than CVE-2017-8535, CVE-2017-8536, CVE-2017-8537, and CVE-2017-8542.	2017-05-26	not yet calculated	CVE-2017-8539 BID(link is external) CONFIRM(link is external)
microsoft -- malware_protection_engine	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka "Microsoft Malware Protection Engine Denial of Service Vulnerability", a different vulnerability than CVE-2017-8536, CVE-2017-8537, CVE-2017-8539, and CVE-2017-8542.	2017-05-26	not yet calculated	CVE-2017-8535 BID(link is external) CONFIRM(link is external)
microsoft -- malware_protection_engine	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka "Microsoft Malware Protection Engine Denial of Service Vulnerability", a different vulnerability than CVE-2017-8535, CVE-2017-8537, CVE-2017-8539, and CVE-2017-8542.	2017-05-26	not yet calculated	CVE-2017-8536 BID(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- malware_protection_engine	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka "Microsoft Malware Protection Engine Denial of Service Vulnerability", a different vulnerability than CVE-2017-8535, CVE-2017-8536, CVE-2017-8537, and CVE-2017-8539.	2017-05-26	not yet calculated	CVE-2017-8542 BID(link is external) CONFIRM(link is external)
moxa -- oncell	A Plaintext Storage of a Password issue was discovered in Moxa OnCell G3110-HSPA Version 1.3 build 15082117 and previous versions, OnCell G3110-HSDPA Version 1.2 Build 09123015 and previous versions, OnCell G3150-HSDPA Version 1.4 Build 11051315 and previous versions, OnCell 5104-HSDPA, OnCell 5104-HSPA, and OnCell 5004-HSPA. The application's configuration file contains parameters that represent passwords in plaintext.	2017-05-29	not yet calculated	CVE-2017-7913 MISC
moxa -- oncell	A Cross-Site Request Forgery issue was discovered in Moxa OnCell G3110-HSPA Version 1.3 build 15082117 and previous versions, OnCell G3110-HSDPA Version 1.2 Build 09123015 and previous versions, OnCell G3150-HSDPA Version 1.4 Build 11051315 and previous versions, OnCell 5104-HSDPA, OnCell 5104-HSPA, and OnCell 5004-HSPA. The application does not sufficiently verify if a request was intentionally provided by the user who submitted the request, which could allow an attacker to modify the configuration of the device.	2017-05-29	not yet calculated	CVE-2017-7917 MISC
moxa -- oncell	An Improper Restriction of Excessive Authentication Attempts issue was discovered in Moxa OnCell G3110-HSPA Version 1.3 build 15082117 and previous versions, OnCell G3110-HSDPA Version 1.2 Build 09123015 and	2017-05-29	not yet calculated	CVE-2017-7915 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	previous versions, OnCell G3150-HSDPA Version 1.4 Build 11051315 and previous versions, OnCell 5104-HSDPA, OnCell 5104-HSPA, and OnCell 5004-HSPA. An attacker can freely use brute force to determine parameters needed to bypass authentication.			
netgear -- wnr2000_devices	NETGEAR WNR2000v3 devices before 1.1.2.14, WNR2000v4 devices before 1.0.0.66, and WNR2000v5 devices before 1.0.0.42 allow authentication bypass and remote code execution via a buffer overflow that uses a parameter in the administration webapp. The NETGEAR ID is PSV-2016-0261.	2017-05-26	not yet calculated	CVE-2017-6862 BID(link is external) CONFIRM(link is external)
nss -- nss	Null pointer dereference vulnerability in NSS since 3.24.0 was found when server receives empty SSLv2 messages resulting into denial of service by remote attacker.	2017-05-30	not yet calculated	CVE-2017-7502 BID(link is external) CONFIRM
open_ticket_request_system -- open_ticket_request_system	Open Ticket Request System (OTRS) 3.3.9 has XSS in index.pl?Action=AgentStats requests, as demonstrated by OrderBy=[XSS] and Direction=[XSS] attacks.	2017-05-29	not yet calculated	CVE-2017-9299 MISC(link is external)
openemr -- openemr	OpenEMR 5.0.0 and prior allows low-privilege users to upload files of dangerous types which can result in arbitrary code execution within the context of the vulnerable application.	2017-06-02	not yet calculated	CVE-2017-9380 MISC(link is external)
openldap -- openldap	servers/slapd/back-mdb/search.c in OpenLDAP through 2.4.44 is prone to a double free vulnerability. A user with access to search the directory can crash slapd by issuing a search including the Paged Results control with a page size of 0.	2017-05-29	not yet calculated	CVE-2017-9287 CONFIRM BID(link is external) CONFIRM
palo_alto_networks -- panorama_vm_appliance	Palo Alto Networks Panorama VM Appliance with PAN-OS before 6.0.1 might allow remote attackers to execute arbitrary Python code via a crafted firmware image file.	2017-06-01	not yet calculated	CVE-2015-6531 BID(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
perl -- perl	Race condition in the rmtree and remove_tree functions in the File-Path module before 2.13 for Perl allows attackers to set the mode on arbitrary files via vectors involving directory-permission loosening logic.	2017-06-01	not yet calculated	CVE-2017-6512 CONFIRM CONFIRM
phoenix_broadband_technologies -- poweragent_sc3_bms	A Use of Hard-Coded Password issue was discovered in Phoenix Broadband PowerAgent SC3 BMS, all versions prior to v6.87. Use of a hard-coded password may allow unauthorized access to the device.	2017-06-02	not yet calculated	CVE-2017-6039 MISC
pivotx -- pivotx	PivotX 2.3.11 allows remote authenticated users to execute arbitrary PHP code via vectors involving an upload of a .htaccess file.	2017-05-31	not yet calculated	CVE-2017-8402 MISC(link is external)
poppler -- poppler	In Poppler 0.54.0, a memory leak vulnerability was found in the function Object::initArray in Object.cc, which allows attackers to cause a denial of service via a crafted file.	2017-06-02	not yet calculated	CVE-2017-9408 CONFIRM
poppler -- poppler	In Poppler 0.54.0, a memory leak vulnerability was found in the function gmalloc in gmem.cc, which allows attackers to cause a denial of service via a crafted file.	2017-06-02	not yet calculated	CVE-2017-9406 CONFIRM
poppler -- poppler	poppler since version 0.17.3 has been vulnerable to NULL pointer dereference in pdfunite triggered by specially crafted documents.	2017-05-30	not yet calculated	CVE-2017-7511 CONFIRM
qemu -- qemu	Memory leak in the virtio_gpu_set_scanout function in hw/display/virtio-gpu.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (memory consumption) via a large number of "VIRTIO_GPU_CMD_SET_SCANOUT:" commands.	2017-06-01	not yet calculated	CVE-2017-9060 CONFIRM MLIST(link is external) MISC(link is external)
realnetworks -- realplayer	RealPlayer 16.0.2.32 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted mp4 file.	2017-05-29	not yet calculated	CVE-2017-9302 MISC(link is external) BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
samba -- samba	Samba since version 3.5.0 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.	2017-05-30	not yet calculated	CVE-2017-7494 BID(link is external) CONFIRM
samsung -- syncthru_admin_6	Multiple directory traversal vulnerabilities in Samsung SyncThru 6 before 1.0 allow remote attackers to delete arbitrary files via unspecified parameters to (1) upload/updateDriver or (2) upload/addDriver or to execute arbitrary code with SYSTEM privileges via unspecified parameters to (3) uploadCloning.html, (4) fileupload.html, (5) uploadFirmware.html, or (6) upload/driver.	2017-06-01	not yet calculated	CVE-2015-5473 BID(link is external) MISC(link is external) MISC(link is external) MISC(link is external) MISC(link is external) MISC(link is external) MISC(link is external)
soffid -- soffid_iam	Untrusted Java serialization in Soffid IAM console before 1.7.5 allows remote attackers to achieve arbitrary remote code execution via a crafted authentication request.	2017-06-02	not yet calculated	CVE-2017-9363 CONFIRM(link is external)
telaxus -- epesi	The Agenda component in Telaxus EPESI 1.8.2 and earlier has a Stored Cross-site Scripting (XSS) vulnerability in modules/Utils/RecordBrowser/RecordBrowserCommon_0.php, which allows remote attackers to inject arbitrary web script or HTML via a crafted meeting description parameter.	2017-06-01	not yet calculated	CVE-2017-9331 CONFIRM(link is external) CONFIRM(link is external)
telaxus -- epesi	Telaxus EPESI 1.8.2 and earlier has a Stored Cross-site Scripting (XSS) vulnerability in modules/Base/Dashboard/Dashboard_0.php, which allows remote attackers to inject arbitrary web script or HTML via a crafted tab_name parameter.	2017-06-02	not yet calculated	CVE-2017-9366 CONFIRM(link is external) CONFIRM(li

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				nk is external)
the_foreman -- the_foreman	Foreman since version 1.5 is vulnerable to an incorrect authorization check due to which users with user management permission who are assigned to some organization(s) can do all operations granted by these permissions on all administrator user object outside of their scope, such as editing global admin accounts including changing their passwords.	2017-05-26	not yet calculated	CVE-2017-7505 CONFIRM BID(link is external) CONFIRM(link is external)
tiki_software -- tiki_wiki_cms_groupware	lib/core/TikiFilter/PreventXss.php in Tiki Wiki CMS Groupware 16.2 allows remote attackers to bypass the XSS filter via padded zero characters, as demonstrated by an attack on tiki-batch_send_newsletter.php.	2017-05-31	not yet calculated	CVE-2017-9305 MISC(link is external) MISC(link is external)
videolan_organization -- videolan_vlc_media_player	plugins\audio_filter\libmpgatofixed32_plugin.dll in VideoLAN VLC media player 2.2.4 allows remote attackers to cause a denial of service (invalid read and application crash) or possibly have unspecified other impact via a crafted file.	2017-05-29	not yet calculated	CVE-2017-9301 MISC(link is external) BID(link is external)
videolan_organization -- videolan_vlc_media_player	plugins\codec\libflac_plugin.dll in VideoLAN VLC media player 2.2.4 allows remote attackers to cause a denial of service (heap corruption and application crash) or possibly have unspecified other impact via a crafted FLAC file.	2017-05-29	not yet calculated	CVE-2017-9300 MISC(link is external) BID(link is external)
vmware -- horizon_daas	VMware Horizon DaaS before 7.0.0 contains a vulnerability that exists due to insufficient validation of data. An attacker may exploit this issue by tricking DaaS client users into connecting to a malicious server and sharing all their drives and devices. Successful exploitation of this vulnerability requires a victim to download a specially crafted RDP file through DaaS client by clicking on a malicious link.	2017-05-31	not yet calculated	CVE-2017-4897 BID(link is external) CONFIRM(link is external)
websitebaker -- websitebaker	WebsiteBaker v2.10.0 has a stored XSS vulnerability in /account/details.php.	2017-06-02	not yet calculated	CVE-2017-9361

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC(link is external)
websitebaker -- websitebaker	WebsiteBaker v2.10.0 has a SQL injection vulnerability in /account/details.php.	2017-06-02	not yet calculated	CVE-2017-9360 MISC(link is external)
wireshark_foundation -- wireshark	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the openSAFETY dissector could crash or exhaust system memory. This was addressed in epan/dissectors/packet-opensafety.c by checking for a negative length.	2017-06-02	not yet calculated	CVE-2017-9350 MISC MISC MISC MISC
wireshark_foundation -- wireshark	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the DNS dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-dns.c by trying to detect self-referencing pointers.	2017-06-02	not yet calculated	CVE-2017-9345 MISC MISC MISC MISC
wireshark_foundation -- wireshark	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the Bluetooth L2CAP dissector could divide by zero. This was addressed in epan/dissectors/packet-btl2cap.c by validating an interval value.	2017-06-02	not yet calculated	CVE-2017-9344 MISC MISC MISC MISC
wireshark_foundation -- wireshark	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the MSNIP dissector misuses a NULL pointer. This was addressed in epan/dissectors/packet-msnip.c by validating an IPv4 address.	2017-06-02	not yet calculated	CVE-2017-9343 MISC MISC MISC MISC
wireshark_foundation -- wireshark	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the Bazaar dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-bzr.c by ensuring that backwards parsing cannot occur.	2017-06-02	not yet calculated	CVE-2017-9352 MISC MISC MISC
wireshark_foundation -- wireshark	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the SoulSeek dissector could go into an infinite loop. This was addressed in	2017-06-02	not yet calculated	CVE-2017-9346 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	epan/dissectors/packet-slsk.c by making loop bounds more explicit.			MISC MISC
wireshark_foundation -- wireshark	In Wireshark 2.2.0 to 2.2.6, the IPv6 dissector could crash. This was addressed in epan/dissectors/packet-ipv6.c by validating an IPv6 address.	2017-06-02	not yet calculated	CVE-2017-9353 MISC MISC MISC MISC
wireshark_foundation -- wireshark	In Wireshark 2.2.0 to 2.2.6, the ROS dissector could crash with a NULL pointer dereference. This was addressed in epan/dissectors/asn1/ros/packet-ros-template.c by validating an OID.	2017-06-02	not yet calculated	CVE-2017-9347 MISC MISC MISC MISC
wireshark_foundation -- wireshark	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the RGMP dissector could crash. This was addressed in epan/dissectors/packet-rgmp.c by validating an IPv4 address.	2017-06-02	not yet calculated	CVE-2017-9354 MISC MISC MISC MISC
wireshark_foundation -- wireshark	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the DICOM dissector has an infinite loop. This was addressed in epan/dissectors/packet-dcm.c by validating a length value.	2017-06-02	not yet calculated	CVE-2017-9349 MISC MISC MISC MISC
wireshark_foundation -- wireshark	In Wireshark 2.2.0 to 2.2.6, the DOF dissector could read past the end of a buffer. This was addressed in epan/dissectors/packet-dof.c by validating a size value.	2017-06-02	not yet calculated	CVE-2017-9348 MISC MISC MISC MISC
wireshark_foundation -- wireshark	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the DHCP dissector could read past the end of a buffer. This was addressed in epan/dissectors/packet-bootp.c by extracting the Vendor Class Identifier more carefully.	2017-06-02	not yet calculated	CVE-2017-9351 MISC MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Raygun4WP plugin 1.8.0 for WordPress is vulnerable to a reflected XSS in sendtesterror.php (backurl parameter).	2017-05-29	not yet calculated	CVE-2017-9288 MISC(link is external) MISC(link is external) MISC(link is external)
wordpress -- wordpress	The WP Editor.MD plugin 1.6 for WordPress has a stored XSS vulnerability in the content of a post.	2017-06-01	not yet calculated	CVE-2017-9336 MISC(link is external)
wordpress -- wordpress	The Markdown on Save Improved plugin 2.5 for WordPress has a stored XSS vulnerability in the content of a post.	2017-06-01	not yet calculated	CVE-2017-9337 MISC(link is external)
yara -- yara	libyara/re.c in the regexp module in YARA 3.5.0 allows remote attackers to cause a denial of service (stack consumption) via a crafted rule that is mishandled in the _yr_re_emit function.	2017-05-31	not yet calculated	CVE-2017-9304 CONFIRM(link is external) CONFIRM(link is external)
zulip -- zulip_server	Zulip Server 1.5.1 and below suffer from an error in the implementation of the invite_by_admins_only setting in the Zulip group chat application server that allowed an authenticated user to invite other users to join a Zulip organization even if the organization was configured to prevent this.	2017-06-02	not yet calculated	CVE-2017-0896 MISC(link is external) MLIST(link is external) MISC(link is external)