Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Adobe					
Connect					
NA	17-07-2017	5	Adobe Connect versions 9.6.1 and earlier have a clickjacking vulnerability. Successful exploitation could lead to a clickjacking attack. **CVE ID: CVE-2017-3101**	NA	A-ADO-CONNE--010817/01
Ansible					
Ansible					
Gain Information	21-07-2017	5	Ansible versions 2.2.3 and earlier are vulnerable to an information disclosure flaw due to the interaction of call back plugins and the no_log directive where the information may not be sanitized properly. **CVE ID: CVE-2017-7473**	https://github.com/ansible/ansible/issues/22505	A-ANS-ANSIB--010817/02
Apache					
Activemq Artemis					
NA	25-07-2017	7.5	XML external entity (XXE) vulnerability in the XPath selector component in Artemis ActiveMQ before commit 48d9951d879e0c8cbb59d4b64ab59d53ef88310d allows remote attackers to have unspecified impact via unknown vectors. **CVE ID: CVE-2015-3208**	https://github.com/apache/activemq-artemis/commit/48d9951d879e0c8cbb59d4b64ab59d53ef88310d	A-APA-ACTIV--010817/03
Openmeetings					
NA	17-07-2017	5	Apache OpenMeetings 1.0.0 updates user password in insecure manner. **CVE ID: CVE-2017-7688**	NA	A-APA-OPENM--010817/04
NA	17-07-2017	5	Apache OpenMeetings 1.0.0 responds to the following insecure HTTP methods: PUT, DELETE, HEAD, and PATCH. **CVE ID: CVE-2017-7685**	NA	A-APA-OPENM--010817/05
DoS	17-07-2017	5	Apache OpenMeetings 1.0.0 doesn't check contents of files being uploaded.	NA	A-APA-OPENM--

			An attacker can cause a denial of service by uploading multiple large files to the server. **CVE ID: CVE-2017-7684**		010817/06
Gain Information	17-07-2017	5	Apache OpenMeetings 1.0.0 displays Tomcat version and detailed error stack trace, which is not secure. **CVE ID: CVE-2017-7683**	http://markmail.org/message/hint6fp66lijqdvu	A-APA-OPENM--010817/07
NA	17-07-2017	5	Apache OpenMeetings 1.0.0 has an overly permissive crossdomain.xml file. This allows for flash content to be loaded from untrusted domains. **CVE ID: CVE-2017-7680**	http://markmail.org/message/whhibri7ervbjvda	A-APA-OPENM--010817/08
NA	17-07-2017	5	Apache OpenMeetings 1.0.0 uses not very strong cryptographic storage, captcha is not used in registration and forget password dialogs and auth forms missing brute force protection. **CVE ID: CVE-2017-7673**	NA	A-APA-OPENM--010817/09
NA	17-07-2017	6.4	Apache OpenMeetings 3.2.0 is vulnerable to parameter manipulation attacks, as a result attacker has access to restricted areas. **CVE ID: CVE-2017-7682**	http://markmail.org/message/dbrbvf5k343ulivf	A-APA-OPENM--010817/10
Sql	17-07-2017	6.5	Apache OpenMeetings 1.0.0 is vulnerable to SQL injection. This allows authenticated users to modify the structure of the existing query and leak the structure of other queries being made by the application in the back-end. **CVE ID: CVE-2017-7681**	http://markmail.org/message/j774dp5ro5xmkmg6	A-APA-OPENM--010817/11
XSS; CSRF	17-07-2017	6.8	Apache OpenMeetings 1.0.0 is vulnerable to Cross-Site Request Forgery (CSRF) attacks, XSS attacks, click-jacking, and MIME based attacks. **CVE ID: CVE-2017-7666**	http://markmail.org/message/fkesu4e5hhz5xdbg	A-APA-OPENM--010817/12
NA	17-07-2017	7.5	Uploaded XML documents were not correctly validated in Apache OpenMeetings 3.1.0. **CVE ID: CVE-2017-7664**	NA	A-APA-OPENM--010817/13
Roller					
Execute Code	17-07-2017	6.5	The weblog page template in Apache Roller 5.1 through 5.1.1 allows remote authenticated users with admin privileges for a weblog to execute arbitrary Java code via crafted Velocity	https://mail-archives.apache.org/mod_mbox/ro	A-APA-ROLLE--010817/14

			Text Language (aka VTL). **CVE ID: CVE-2015-0249**	ller-user/20150 3.mbox/%3 CCAF1aazA PWTduVhr Pr7WiFaspF dsh21yf0Yi SB3UmLjtD VGnfXw@m ail.gmail.co m%3E	
Sling					
XSS	19-07-2017	7.5	In the XSS Protection API module before 1.0.12 in Apache Sling, the method XSS.getValidXML() uses an insecure SAX parser to validate the input string, which allows for XXE attacks in all scripts which use this method to validate user input, potentially allowing an attacker to read sensitive data on the filesystem, perform same-site-request-forgery (SSRF), port-scanning behind the firewall or DoS the application. **CVE ID: CVE-2016-6798**	NA	A-APA-SLING--010817/15
Apple					
Itunes					
Execute Code	20-07-2017	9.3	An issue was discovered in certain Apple products. iTunes before 12.6.2 on Windows is affected. The issue involves the "iTunes" component. It allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID: CVE-2017-7053**	https://support.apple.com/HT207928	A-APP-ITUNE--010817/16
Appsec-labs					
Appsec Labs					
NA	25-07-2017	7.2	AppUse 4.0 allows shell command injection via a proxy field. **CVE ID: CVE-2017-11566**	https://gist.github.com/shiham101/4807e3dea54ee0f0456c47fcd1400e97	A-APP-APPSE--010817/17
Atutor					
Atutor					
Directory Traversal	22-07-2017	5	Directory Traversal exists in ATutor before 2.2.2 via the icon parameter to	NA	A-ATU-ATUTO--

			/mods/_core/courses/users/create_course.php. The attacker can read an arbitrary file by visiting get_course_icon.php?id= after the traversal attack. **CVE ID: CVE-2016-10400**		010817/18
NA	17-07-2017	7.5	ATutor versions 2.2.1 and earlier are vulnerable to a incorrect access control check vulnerability in the Social Application component resulting in privilege escalation. ATutor versions 2.2.1 and earlier are vulnerable to a incorrect access control check vulnerability in the Module component resulting in privilege escalation. ATutor versions 2.2.1 and earlier are vulnerable to a incorrect access control check vulnerability in the Alternative Content component resulting in privilege escalation. **CVE ID: CVE-2017-1000003**	http://www.atutor.ca/atutor/mantis/changelog_page.php?version_id=55	A-ATU-ATUTO--010817/19
Execute Code; Directory Traversal; Bypass	17-07-2017	7.5	ATutor versions 2.2.1 and earlier are vulnerable to a directory traversal and file extension check bypass in the Course component resulting in code execution. ATutor versions 2.2.1 and earlier are vulnerable to a directory traversal vulnerability in the Course Icon component resulting in information disclosure. **CVE ID: CVE-2017-1000002**	http://www.atutor.ca/atutor/mantis/changelog_page.php?version_id=55	A-ATU-ATUTO--010817/20
Audacity					
Audacity					
Execute Code	17-07-2017	6.8	Audacity version 2.1.2 is vulnerable to Dll HIjacking in the avformat-55.dll resulting arbitrary code execution **CVE ID: CVE-2017-1000010**	https://packetstormsecurity.com/files/140365/Audacity-2.1.2-DLL-Hijacking.html	A-AUD-AUDAC--010817/21
Cacti					
Cacti					
Execute Code; SQL Injection	17-07-2017	6.5	SQL injection vulnerability in graph_templates_inputs.php in Cacti 0.8.8b allows remote attackers to	https://www.trustwave.com/Reso	A-CAC-CACTI--010817/

			execute arbitrary SQL commands via the graph_template_input_id and graph_template_id parameters. **CVE ID: CVE-2017-1000031**	urces/Security-Advisories/Advisories/TWSL2016-007/?fid=7789	22
Cairographics					
Cairo					
DoS	17-07-2017	5	cairo-truetype-subset.c in cairo 1.15.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) because of mishandling of an unexpected malloc(0) call. **CVE ID: CVE-2017-9814**	https://bugs.freedesktop.org/show_bug.cgi?id=101547	A-CAI-CAIRO--010817/23
Call-cc					
Chicken					
NA	17-07-2017	5	Due to an incomplete fix for CVE-2012-6125, all versions of CHICKEN Scheme up to and including 4.12.0 are vulnerable to an algorithmic complexity attack. An attacker can provide crafted input which, when inserted into the symbol table, will result in O(n) lookup time. **CVE ID: CVE-2017-11343**	http://lists.gnu.org/archive/html/chicken-announce/2017-07/msg00000.html	A-CAL-CHICK--010817/24
Candlepinproject					
Candlepin					
Gain Information	25-07-2017	6.4	Candlepin allows remote attackers to obtain sensitive information by obtaining Java exception statements as a result of excessive web traffic. **CVE ID: CVE-2015-5187**	https://bugzilla.redhat.com/show_bug.cgi?id=1252147	A-CAN-CANDL--010817/25
Chef Project					
Mixlib-archive					
Directory Traversal	17-07-2017	5	Chef Software's mixlib-archive versions 0.3.0 and older are vulnerable to a directory traversal attack allowing attackers to overwrite arbitrary files by using ".." in tar archive entries **CVE ID: CVE-2017-1000026**	https://github.com/chef/mixlib-archive/blob/master/CHANGELOG.md	A-CHE-MIXLI--010817/26
Chitora					
Lhaz					
Gain Privileges	17-07-2017	9.3	Untrusted search path vulnerability in Self-extracting archive files created by	http://chitora.com/jvn2	A-CHI-LHAZ--

			Lhaz version 2.4.0 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2247**	1369452.html	010817/27
Gain Privileges	17-07-2017	9.3	Untrusted search path vulnerability in Installer of Lhaz version 2.4.0 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2246**	http://chitora.com/jvn21369452.html	A-CHI-LHAZ--010817/28
Lhaz+					
Gain Privileges	17-07-2017	9.3	Untrusted search path vulnerability in Self-extracting archive files created by Lhaz+ version 3.4.0 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2249**	http://chitora.com/jvn21369452.html	A-CHI-LHAZ+--010817/29
Gain Privileges	17-07-2017	9.3	Untrusted search path vulnerability in Installer of Lhaz+ version 3.4.0 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2248**	http://chitora.com/jvn21369452.html	A-CHI-LHAZ+--010817/30
Cisco					
Web Security Appliance; Web Security Virtual Appliance					
Bypass	25-07-2017	5	A vulnerability in the web proxy functionality of the Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to forward traffic from the web proxy interface of an affected device to the administrative management interface of an affected device, aka an Access Control Bypass Vulnerability. Affected Products: virtual and hardware versions of Cisco Web Security Appliance (WSA). More Information: CSCvd88863. Known Affected Releases: 10.1.0-204 9.0.0-485. **CVE ID: CVE-2017-6751**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-wsa5	A-CIS-WEB S--010817/31
NA	25-07-2017	5	A vulnerability in AsyncOS for the Cisco Web Security Appliance (WSA) could allow an unauthenticated, local attacker to log in to the device with the privileges of a limited user or an unauthenticated, remote attacker to authenticate to certain areas of the web	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-WEB S--010817/32

			GUI, aka a Static Credentials Vulnerability. Affected Products: virtual and hardware versions of Cisco Web Security Appliance (WSA). More Information: CSCve06124. Known Affected Releases: 10.1.0-204. Known Fixed Releases: 10.5.1-270. **CVE ID: CVE-2017-6750**	20170719-wsa4	
NA	25-07-2017	7.2	A vulnerability in the CLI parser of the Cisco Web Security Appliance (WSA) could allow an authenticated, local attacker to perform command injection and elevate privileges to root. The attacker must authenticate with valid operator-level or administrator-level credentials. Affected Products: virtual and hardware versions of Cisco Web Security Appliance (WSA). More Information: CSCvd88855. Known Affected Releases: 10.1.0-204. Known Fixed Releases: 10.5.1-270 10.1.1-234. **CVE ID: CVE-2017-6748**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-wsa2	A-CIS-WEB S--010817/33
Webex Event Center;Webex Meeting Center;Webex Meetings;Webex Meetings Server;Webex Meetings Server 2.0;Webex Meetings Server 2.0 Mr8 Patch;Webex Meetings Server 2.0 Mr9 Patch;Webex Meetings Server 2.5;Webex Meetings Server 2.5 Mr2 Patch;Webex Meetings Server 2.5 Mr5 Patch;Webex Meetings Server 2.5 Mr6 Patch;Webex Meetings Server 2.6;Webex Meetings Server 2.6 Mr1 Patch;Webex Meetings Server 2.6 Mr2 Patch;Webex Meetings Server 2.6 Mr3 Patch;Webex Meetings Server 2.7;Webex Meetings Server 2.7 Mr1 Patch;Webex Meetings Server 2.7 Mr2 Patch;Webex Support Center;Webex Training Center					
Execute Code; Overflow	25-07-2017	9.3	A vulnerability in Cisco WebEx browser extensions for Google Chrome and Mozilla Firefox could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server, Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center), and Cisco WebEx Meetings when they are running on Microsoft Windows. The vulnerability is due to a design defect in the extension. An attacker who can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170717-webex	A-CIS-WEBEX--010817/34

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

			affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser. The following versions of the Cisco WebEx browser extensions are affected: Versions prior to 1.0.12 of the Cisco WebEx extension on Google Chrome, Versions prior to 1.0.12 of the Cisco WebEx extension on Mozilla Firefox. Cisco Bug IDs: CSCvf15012 CSCvf15020 CSCvf15030 CSCvf15033 CSCvf15036 CSCvf15037. **CVE ID: CVE-2017-6753**		
Citrix					
Netscaler Sd-wan					
Execute Code	20-07-2017	10	Citrix NetScaler SD-WAN devices through v9.1.2.26.561201 allow remote attackers to execute arbitrary shell commands as root via a CGISESSID cookie. On CloudBridge (the former name of NetScaler SD-WAN) devices, the cookie name was CAKEPHP rather than CGISESSID. **CVE ID: CVE-2017-6316**	NA	A-CIT-NETSC--010817/35
Cloud Foundary					
Capi-release					
Execute Code	24-07-2017	6.8	An issue was discovered in the Cloud Controller API in Cloud Foundry Foundation CAPI-release version 1.33.0 (only). The original fix for CVE-2017-8033 included in CAPI-release 1.33.0 introduces a regression that allows a space developer to execute arbitrary code on the Cloud Controller VM by pushing a specially crafted application. **CVE ID: CVE-2017-8036**	https://www.cloudfoundry.org/CVE-2017-8036/	A-CLO-CAPI---010817/36
Capi-release; Cf-release					
Gain Information	25-07-2017	5	An issue was discovered in the Cloud Controller API in Cloud Foundry Foundation CAPI-release versions after v1.6.0 and prior to v1.35.0 and cf-release versions after v244 and prior to v268. A carefully crafted CAPI request from a Space Developer can allow them to gain access to files on the Cloud	https://www.cloudfoundry.org/CVE-2017-8035/	A-CLO-CAPI---010817/37

			Controller VM for that installation. **CVE ID: CVE-2017-8035**		
Directory Traversal	25-07-2017	6.8	An issue was discovered in the Cloud Controller API in Cloud Foundry Foundation CAPI-release versions prior to v1.35.0 and cf-release versions prior to v268. A filesystem traversal vulnerability exists in the Cloud Controller that allows a space developer to escalate privileges by pushing a specially crafted application that can write arbitrary files to the Cloud Controller VM. **CVE ID: CVE-2017-8033**	https://www.cloudfoundry.org/CVE-2017-8033/	A-CLO-CAPI---010817/38
Capi-release; Cf-release; Routing-release					
NA	17-07-2017	6	The Cloud Controller and Router in Cloud Foundry (CAPI-release capi versions prior to v1.32.0, Routing-release versions prior to v0.159.0, CF-release versions prior to v267) do not validate the issuer on JSON Web Tokens (JWTs) from UAA. With certain multi-zone UAA configurations, zone administrators are able to escalate their privileges. **CVE ID: CVE-2017-8034**	https://www.cloudfoundry.org/CVE-2017-8034/	A-CLO-CAPI---010817/39
Contao					
Contao Cms					
Directory Traversal	21-07-2017	6.5	Contao before 3.5.28 and 4.x before 4.4.1 allows remote attackers to include and execute arbitrary local PHP files via a crafted parameter in a URL, aka Directory Traversal. **CVE ID: CVE-2017-10993**	https://contao.org/en/news/contao-3_5_28.html	A-CON-CONTA--010817/40
Creolabs					
Gravity					
Overflow	17-07-2017	7.5	Creolabs Gravity version 1.0 is vulnerable to a stack overflow in the memcmp function **CVE ID: CVE-2017-1000075**	https://github.com/marcobambini/gravity/issues/133	A-CRE-GRAVI--010817/41
Overflow	17-07-2017	7.5	Creolabs Gravity version 1.0 is vulnerable to a stack overflow in the string_repeat() function. **CVE ID: CVE-2017-1000074**	https://github.com/marcobambini/gravity/issues/131	A-CRE-GRAVI--010817/42

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

Execute Code; Overflow	17-07-2017	7.5	Creolabs Gravity version 1.0 is vulnerable to a heap overflow in an undisclosed component that can result in arbitrary code execution. **CVE ID: CVE-2017-1000073**	https://github.com/marcobambini/gravity/issues/129	A-CRE-GRAVI--010817/43
NA	17-07-2017	7.5	Creolabs Gravity version 1.0 is vulnerable to a Double Free in gravity_value resulting potentially leading to modification of unexpected memory locations **CVE ID: CVE-2017-1000072**	https://github.com/marcobambini/gravity/issues/123	A-CRE-GRAVI--010817/44
Cygwin					
Cygwin					
Overflow	21-07-2017	5	Cygwin versions 1.7.2 up to and including 1.8.0 are vulnerable to buffer overflow vulnerability in wcsxfrm/wcsxfrm_l functions resulting into denial-of-service by crashing the process or potential hijack of the process running with administrative privileges triggered by specially crafted input string. **CVE ID: CVE-2017-7523**	https://cygwin.com/ml/cygwin/2017-05/msg00149.html	A-CYG-CYGWI--010817/45
Debian					
TOR					
Bypass	23-07-2017	5	debian/tor.init in the Debian tor_0.2.9.11-1~deb9u1 package for Tor was designed to execute aa-exec from the standard system pathname if the apparmor package is installed, but implements this incorrectly (with a wrong assumption that the specific pathname would remain the same forever), which allows attackers to bypass intended AppArmor restrictions by leveraging the silent loss of this protection mechanism. NOTE: this does not affect systems, such as default Debian stretch installations, on which Tor startup relies on a systemd unit file (instead of this tor.init script). **CVE ID: CVE-2017-11565**	https://bugs.debian.org/869153	A-DEB-TOR--010817/46
Docker					
Docker Registry					
DoS	20-07-2017	5	Docker Registry before 2.6.2 in Docker Distribution does not properly restrict	https://github.com/doc	A-DOC-DOCKE--

			the amount of content accepted from a user, which allows remote attackers to cause a denial of service (memory consumption) via the manifest endpoint. **CVE ID: CVE-2017-11468**	ker/distribution/releases/tag/v2.6.2	010817/47
Dotcms					
Dotcms					
Execute Code; Directory Traversal	19-07-2017	9	Arbitrary file upload vulnerability in com/dotmarketing/servlets/AjaxFileUploadServlet.class in dotCMS 4.1.1 allows remote authenticated administrators to upload .jsp files to arbitrary locations via directory traversal sequences in the fieldName parameter to servlets/ajax_file_upload. This results in arbitrary code execution by requesting the .jsp file at a /assets URI. **CVE ID: CVE-2017-11466**	NA	A-DOT-DOTCM--010817/48
Dotnetnuke					
Dotnetnuke					
Execute Code	20-07-2017	6.5	DNN (aka DotNetNuke) before 9.1.1 has Remote Code Execution via a cookie, aka "2017-08 (Critical) Possible remote code execution on DNN sites." **CVE ID: CVE-2017-9822**	http://www.dnnsoftware.com/community/security/security-center	A-DOT-DOTNE--010817/49
EMC					
M&R; Storage M&r; Vipr Srm; Vnx M&r					
NA	17-07-2017	10	EMC ViPR SRM, EMC Storage M&R, EMC VNX M&R, EMC M&R for SAS Solution Packs (EMC ViPR SRM prior to 4.1, EMC Storage M&R prior to 4.1, EMC VNX M&R all versions, EMC M&R (Watch4Net) for SAS Solution Packs all versions) contain undocumented accounts with default passwords for Webservice Gateway and RMI JMX components. A remote attacker with the knowledge of the default password may potentially use these accounts to run arbitrary web service and remote procedure calls on the affected system. **CVE ID: CVE-2017-8011**	http://seclists.org/fulldisclosure/2017/Jul/21	A-EMC-M&R;S--010817/50
Rsa Identity Governance And Lifecycle; Rsa Identity Management And Governance; Rsa Via Lifecycle And Governance					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

Execute Code	17-07-2017	6.5	The EMC RSA Identity Governance and Lifecycle, RSA Via Lifecycle and Governance and RSA IMG products (RSA Identity Governance and Lifecycle versions 7.0.1, 7.0.2, all patch levels; RSA Via Lifecycle and Governance version 7.0, all patch levels; RSA Identity Management and Governance (RSA IMG) versions 6.9.1, all patch levels) allow an application administrator to upload arbitrary files that may potentially contain a malicious code. The malicious file could be then executed on the affected system with the privileges of the user the application is running under. **CVE ID: CVE-2017-8004**	http://seclists.org/fulldisclosure/2017/Jul/24	A-EMC-RSA I--010817/51
Exiv2					
Exiv2					
DoS	22-07-2017	5	There is an illegal address access in the extend_alias_table function in localealias.c of Exiv2 0.26. A crafted input will lead to remote denial of service. **CVE ID: CVE-2017-11553**	https://bugzilla.redhat.com/show_bug.cgi?id=1471772	A-EXI-EXIV2--010817/52
Denial of Service; Overflow; Memory Corruption	23-07-2017	5	There is a Mismatched Memory Management Routines vulnerability in the Exiv2::FileIo::seek function of Exiv2 0.26 that will lead to a remote denial of service attack (heap memory corruption) via crafted input. **CVE ID: CVE-2017-11592**	https://bugzilla.redhat.com/show_bug.cgi?id=1473889	A-EXI-EXIV2--010817/53
DoS	23-07-2017	5	There is a Floating point exception in the Exiv2::ValueType function in Exiv2 0.26 that will lead to a remote denial of service attack via crafted input. **CVE ID: CVE-2017-11591**	https://bugzilla.redhat.com/show_bug.cgi?id=1473888	A-EXI-EXIV2--010817/54
Eyesofnetwork					
Eyesofnetwork					
Sql	17-07-2017	10	EyesOfNetwork (EON) 5.1 Unauthenticated SQL Injection in eonweb leading to remote root **CVE ID: CVE-2017-1000060**	https://riorau.github.io/pentest/web/2017/03/28/from-unauthenticated-to-	A-EYE-EYESO--010817/55

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

				root-supervision.html	
Fedoraproject					
Fedmsg					
NA	17-07-2017	5	FedMsg 0.18.1 and older is vulnerable to a message validation flaw resulting in message validation not being enabled if configured to be on. **CVE ID: CVE-2017-1000001**	https://github.com/fedora-infra/fedmsg/blob/0.18.2/CHANGELOG.rst	A-FED-FEDMS--010817/56
Ffmpeg					
Ffmpeg					
Denial of Service; Overflow	17-07-2017	6.8	Integer overflow in the ape_decode_frame function in libavcodec/apedec.c in FFmpeg through 3.3.2 allows remote attackers to cause a denial of service (out-of-array access and application crash) or possibly have unspecified other impact via a crafted APE file. **CVE ID: CVE-2017-11399**	https://github.com/FFmpeg/FFmpeg/commit/ba4beaf6149f7241c8bd85fe853318c2f6837ad0	A-FFM-FFMPE--010817/57
Finecms					
Finecms					
NA	23-07-2017	5.8	dayrui FineCms 5.0.9 has URL Redirector Abuse via the url parameter in a sync action, related to controllers/Weixin.php. **CVE ID: CVE-2017-11586**	http://lorexxar.cn/2017/07/20/FineCMS%20multi%20vulnerablity%20before%20v5.0.9/#URL-Redirector-Abuse	A-FIN-FINEC--010817/58
Execute Code	23-07-2017	7.5	dayrui FineCms 5.0.9 has remote PHP code execution via the param parameter in an action=cache request to libraries/Template.php, aka Eval Injection. **CVE ID: CVE-2017-11585**	http://lorexxar.cn/2017/07/20/FineCMS%20multi%20vulnerablity%20before%20v5.0.9/#remote-php-code-	A-FIN-FINEC--010817/59

				execution	
Sql	23-07-2017	7.5	dayrui FineCms 5.0.9 has SQL Injection via the field parameter in an action=module, action=member, action=form, or action=related request to libraries/Template.php. **CVE ID: CVE-2017-11584**	http://lorexxar.cn/2017/07/20/FineCMS%20multi%20vulnerablity%20before%20v5.0.9/#SQL-injection-via-system-field-parameter	A-FIN-FINEC--010817/60
Sql	23-07-2017	7.5	dayrui FineCms 5.0.9 has SQL Injection via the catid parameter in an action=related request to libraries/Template.php. **CVE ID: CVE-2017-11583**	http://lorexxar.cn/2017/07/20/FineCMS%20multi%20vulnerablity%20before%20v5.0.9/#SQL-injection-in-action-related-catid-parameter	A-FIN-FINEC--010817/61
Sql	23-07-2017	7.5	dayrui FineCms 5.0.9 has SQL Injection via the num parameter in an action=related or action=tags request to libraries/Template.php. **CVE ID: CVE-2017-11582**	http://lorexxar.cn/2017/07/20/FineCMS%20multi%20vulnerablity%20before%20v5.0.9/#SQL-injection-after-limit-via-system-num-parameter	A-FIN-FINEC--010817/62
Fiyo					
Fiyo Cms					
Directory Traversal	26-07-2017	5	dapur\apps\app_config\controller\backuper.php in Fiyo CMS 2.0.7 allows remote attackers to delete arbitrary	https://github.com/FiyoCMS/Fiyo	A-FIY-FIYO --010817/

			files via directory traversal sequences in the file parameter in a type=database request, a different vulnerability than CVE-2017-8853. **CVE ID: CVE-2017-11630**	CMS/issues/6	63
Sql	17-07-2017	7.5	Fiyo CMS v2.0.7 has an SQL injection vulnerability in dapur/apps/app_article/sys_article.php via the name parameter in editing or adding a tag name. **CVE ID: CVE-2017-11354**	https://github.com/FiyoCMS/FiyoCMS/issues/4	A-FIY-FIYO --010817/64
Sql	18-07-2017	7.5	Fiyo CMS 2.0.7 has SQL injection in /apps/app_article/controller/editor.php via $_POST['id'] and $_POST['art_title']. **CVE ID: CVE-2017-11419**	https://github.com/FiyoCMS/FiyoCMS/issues/5	A-FIY-FIYO --010817/65
Sql	18-07-2017	7.5	Fiyo CMS 2.0.7 has SQL injection in dapur/apps/app_article/controller/article_list.php via $_GET['cat'], $_GET['user'], $_GET['level'], and $_GET['iSortCol_'.$i]. **CVE ID: CVE-2017-11418**	https://github.com/FiyoCMS/FiyoCMS/issues/5	A-FIY-FIYO --010817/66
Sql	18-07-2017	7.5	Fiyo CMS 2.0.7 has SQL injection in dapur/apps/app_article/controller/article_status.php via $_GET['id']. **CVE ID: CVE-2017-11417**	https://github.com/FiyoCMS/FiyoCMS/issues/5	A-FIY-FIYO --010817/67
Sql	18-07-2017	7.5	Fiyo CMS 2.0.7 has SQL injection in /apps/app_comment/controller/insert.php via the name parameter. **CVE ID: CVE-2017-11416**	https://github.com/FiyoCMS/FiyoCMS/issues/5	A-FIY-FIYO --010817/68
Sql	18-07-2017	7.5	Fiyo CMS 2.0.7 has SQL injection in dapur/apps/app_article/sys_article.php via $_POST['parent_id'], $_POST['desc'], $_POST['keys'], and $_POST['level']. **CVE ID: CVE-2017-11415**	https://github.com/FiyoCMS/FiyoCMS/issues/5	A-FIY-FIYO --010817/69
Sql	18-07-2017	7.5	Fiyo CMS 2.0.7 has SQL injection in dapur/apps/app_comment/sys_comment.php via $_POST['comment'], $_POST['name'], $_POST['web'], $_POST['email'], $_POST['status'], $_POST['id'], and $_REQUEST['id']. **CVE ID: CVE-2017-11414**	https://github.com/FiyoCMS/FiyoCMS/issues/5	A-FIY-FIYO --010817/70
Sql	18-07-2017	7.5	Fiyo CMS 2.0.7 has SQL injection in dapur/apps/app_article/controller/comment_status.php via $_GET['id'].	https://github.com/FiyoCMS/Fiyo	A-FIY-FIYO --010817/

			CVE ID: CVE-2017-11413	CMS/issues/5	71
Sql	18-07-2017	7.5	Fiyo CMS 2.0.7 has SQL injection in dapur/apps/app_comment/controller/comment_status.php via $_GET['id']. **CVE ID: CVE-2017-11412**	https://github.com/FiyoCMS/FiyoCMS/issues/5	A-FIY-FIYO --010817/72
Sql	26-07-2017	7.5	dapur/app/app_user/controller/status.php in Fiyo CMS 2.0.7 has SQL injection via the id parameter. **CVE ID: CVE-2017-11631**	https://github.com/FiyoCMS/FiyoCMS/issues/7	A-FIY-FIYO --010817/73
Fontforge					
Fontforge					
Execute Code; Overflow	23-07-2017	6.8	FontForge 20161012 is vulnerable to a heap-based buffer over-read in readttfcopyrights (parsettf.c) resulting in DoS or code execution via a crafted otf file. **CVE ID: CVE-2017-11569**	https://github.com/fontforge/fontforge/issues/3093	A-FON-FONTF--010817/74
Fontforge Project					
Fontforge					
Execute Code; Overflow	23-07-2017	6.8	FontForge 20161012 is vulnerable to a buffer over-read in getsid (parsettf.c) resulting in DoS or code execution via a crafted otf file. **CVE ID: CVE-2017-11577**	https://github.com/fontforge/fontforge/issues/3088	A-FON-FONTF--010817/75
Execute Code; Overflow	23-07-2017	6.8	FontForge 20161012 is vulnerable to a buffer over-read in strnmatch (char.c) resulting in DoS or code execution via a crafted otf file, related to a call from the readttfcopyrights function in parsettf.c. **CVE ID: CVE-2017-11575**	https://github.com/fontforge/fontforge/issues/3096	A-FON-FONTF--010817/76
Execute Code; Overflow	23-07-2017	6.8	FontForge 20161012 is vulnerable to a heap-based buffer overflow in readcffset (parsettf.c) resulting in DoS or code execution via a crafted otf file. **CVE ID: CVE-2017-11574**	https://github.com/fontforge/fontforge/issues/3090	A-FON-FONTF--010817/77
Execute Code; Overflow	23-07-2017	6.8	FontForge 20161012 is vulnerable to a buffer over-read in ValidatePostScriptFontName (parsettf.c) resulting in DoS or code execution via a crafted otf file. **CVE ID: CVE-2017-11573**	https://github.com/fontforge/fontforge/issues/3098	A-FON-FONTF--010817/78
Execute Code; Overflow	23-07-2017	6.8	FontForge 20161012 is vulnerable to a heap-based buffer over-read in	https://github.com/fon	A-FON-FONTF--

			readcfftopdicts (parsettf.c) resulting in DoS or code execution via a crafted otf file. **CVE ID: CVE-2017-11572**	tforge/fontforge/issues/3092	010817/79
Execute Code; Overflow	23-07-2017	6.8	FontForge 20161012 is vulnerable to a stack-based buffer overflow in addnibble (parsettf.c) resulting in DoS or code execution via a crafted otf file. **CVE ID: CVE-2017-11571**	https://github.com/fontforge/fontforge/issues/3087	A-FON-FONTF--010817/80
Execute Code; Overflow	23-07-2017	6.8	FontForge 20161012 is vulnerable to a buffer over-read in umodenc (parsettf.c) resulting in DoS or code execution via a crafted otf file. **CVE ID: CVE-2017-11570**	https://github.com/fontforge/fontforge/issues/3097	A-FON-FONTF--010817/81
Execute Code; Overflow	23-07-2017	6.8	FontForge 20161012 is vulnerable to a heap-based buffer over-read in PSCharStringToSplines (psread.c) resulting in DoS or code execution via a crafted otf file. **CVE ID: CVE-2017-11568**	https://github.com/fontforge/fontforge/issues/3089	A-FON-FONTF--010817/82
Fortinet					
Fortiwlm					
Execute Code	22-07-2017	7.5	A hard-coded account named 'upgrade' in Fortinet FortiWLM 8.3.0 and lower versions allows a remote attacker to log-in and execute commands with 'upgrade' account privileges. **CVE ID: CVE-2017-7336**	https://fortiguard.com/advisory/FG-IR-17-115	A-FOR-FORTI--010817/83
Framasoft					
Framadate					
Execute Code	17-07-2017	7.5	Framadate version 1.0 is vulnerable to Formula Injection in the CSV Export resulting possible Information Disclosure and Code Execution **CVE ID: CVE-2017-1000039**	https://framagit.org/framasoft/framadate/issues/220	A-FRA-FRAMA--010817/84
Freeradius					
Freeradius					
Denial of Service; Overflow	17-07-2017	5	An FR-GV-304 issue in FreeRADIUS 3.x before 3.0.15 allows "DHCP - Buffer over-read in fr_dhcp_decode_suboptions()" and a denial of service. **CVE ID: CVE-2017-10987**	http://freeradius.org/security/fuzzer-2017.html	A-FRE-FREER--010817/85
DoS	17-07-2017	5	An FR-GV-303 issue in FreeRADIUS 3.x before 3.0.15 allows "DHCP - Infinite read in dhcp_attr2vp()" and a denial of	http://freeradius.org/security/fuzz	A-FRE-FREER--010817/

			service. **CVE ID: CVE-2017-10986**	er-2017.html	86
Denial of Service; Overflow	17-07-2017	5	An FR-GV-206 issue in FreeRADIUS 2.x before 2.2.10 and 3.x before 3.0.15 allows "DHCP - Read overflow when decoding option 63" and a denial of service. **CVE ID: CVE-2017-10983**	http://freeradius.org/security/fuzzer-2017.html	A-FRE-FREER--010817/87
Denial of Service; Overflow	17-07-2017	5	An FR-GV-205 issue in FreeRADIUS 2.x before 2.2.10 allows "DHCP - Buffer over-read in fr_dhcp_decode_options()" and a denial of service. **CVE ID: CVE-2017-10982**	http://freeradius.org/security/fuzzer-2017.html	A-FRE-FREER--010817/88
Denial of Service; Overflow	17-07-2017	5	An FR-GV-204 issue in FreeRADIUS 2.x before 2.2.10 allows "DHCP - Memory leak in fr_dhcp_decode()" and a denial of service. **CVE ID: CVE-2017-10981**	http://freeradius.org/security/fuzzer-2017.html	A-FRE-FREER--010817/89
Denial of Service; Overflow	17-07-2017	5	An FR-GV-203 issue in FreeRADIUS 2.x before 2.2.10 allows "DHCP - Memory leak in decode_tlv()" and a denial of service. **CVE ID: CVE-2017-10980**	http://freeradius.org/security/fuzzer-2017.html	A-FRE-FREER--010817/90
Denial of Service; Overflow	17-07-2017	5	An FR-GV-201 issue in FreeRADIUS 2.x before 2.2.10 and 3.x before 3.0.15 allows "Read / write overflow in make_secret()" and a denial of service. **CVE ID: CVE-2017-10978**	http://freeradius.org/security/fuzzer-2017.html	A-FRE-FREER--010817/91
Denial of Service; Execute Code; Overflow	17-07-2017	7.5	An FR-GV-301 issue in FreeRADIUS 3.x before 3.0.15 allows "Write overflow in data2vp_wimax()" - this allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code. **CVE ID: CVE-2017-10984**	http://freeradius.org/security/fuzzer-2017.html	A-FRE-FREER--010817/92
Denial of Service; Execute Code; Overflow	17-07-2017	7.5	An FR-GV-202 issue in FreeRADIUS 2.x before 2.2.10 allows "Write overflow in rad_coalesce()" - this allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code. **CVE ID: CVE-2017-10979**	http://freeradius.org/security/fuzzer-2017.html	A-FRE-FREER--010817/93
DoS	17-07-2017	7.8	An FR-GV-302 issue in FreeRADIUS 3.x before 3.0.15 allows "Infinite loop and memory exhaustion with 'concat' attributes" and a denial of service. **CVE ID: CVE-2017-10985**	http://freeradius.org/security/fuzzer-2017.html	A-FRE-FREER--010817/94

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

Fujielectric					
V-server					
Execute Code; Overflow; Memory Corruption	17-07-2017	7.5	An issue was discovered in Fuji Electric V-Server Version 3.3.22.0 and prior. A memory corruption vulnerability has been identified (aka improper restriction of operations within the bounds of a memory buffer), which may allow remote code execution. **CVE ID: CVE-2017-9639**	NA	A-FUJ-V-SER--010817/95
Genivia					
Gsoap					
DoS; Execute Code; Overflow	19-07-2017	5.1	Integer overflow in the soap_get function in Genivia gSOAP 2.7.x and 2.8.x before 2.8.48, as used on Axis cameras and other devices, allows remote attackers to execute arbitrary code or cause a denial of service (stack-based buffer overflow and application crash) via a large XML document, aka Devil's Ivy. NOTE: the large document would be blocked by many common web-server configurations on general-purpose computers. **CVE ID: CVE-2017-9765**	NA	A-GEN-GSOAP--010817/96
Geutebrueck					
Gcore					
Execute Code; Overflow	21-07-2017	7.5	Stack-based buffer overflow in GCoreServer.exe in the server in Geutebrueck Gcore 1.3.8.42 and 1.4.2.37 allows remote attackers to execute arbitrary code via a long URI in a GET request. **CVE ID: CVE-2017-11517**	https://www.exploit-db.com/exploits/41153/	A-GEU-GCORE--010817/97
Glpi-project					
Glpi					
CSRF	19-07-2017	6	Cross-Site Request Forgery (CSRF) vulnerability in GLPI 0.90.4 allows remote authenticated attackers to submit a request that could lead to the creation of an admin account in the application. **CVE ID: CVE-2016-7507**	https://github.com/glpi-project/glpi/issues/2483	A-GLP-GLPI--010817/98
Sql	17-07-2017	7.5	GLPI before 9.1.5 allows SQL injection via an ajax/getDropdownValue.php request with an entity_restrict	https://github.com/glpi-	A-GLP-GLPI--010817/

			parameter that is not a list of integers. **CVE ID: CVE-2017-11329**	project/glpi/releases/tag/9.1.5	99
Sql	20-07-2017	7.5	GLPI before 9.1.5.1 has SQL Injection in the condition rule field, exploitable via front/rulesengine.test.php. **CVE ID: CVE-2017-11475**	https://github.com/glpi-project/glpi/issues/2476	A-GLP-GLPI--010817/100
Sql	20-07-2017	7.5	GLPI before 9.1.5.1 has SQL Injection in the $crit variable in inc/computer_softwareversion.class.php, exploitable via ajax/common.tabs.php. **CVE ID: CVE-2017-11474**	https://github.com/glpi-project/glpi/issues/2475	A-GLP-GLPI--010817/101
Gnome					
Gtk-vnc					
Overflow Memory Corruption	17-07-2017	7.5	gtk-vnc 0.4.2 and older doesn't check framebuffer boundaries correctly when updating framebuffer which may lead to memory corruption when rendering **CVE ID: CVE-2017-1000044**	https://git.gnome.org/browse/gtk-vnc/commit/?id=f3fc5e57a78d4be9872f1394f697b9929873a737	A-GNO-GTK-V--010817/102
Librsvg					
NA	19-07-2017	6.8	A SIGFPE is raised in the function box_blur_line of rsvg-filter.c in GNOME librsvg 2.40.17 during an attempted parse of a crafted SVG file, because of incorrect protection against division by zero. **CVE ID: CVE-2017-11464**	https://bugzilla.gnome.org/show_bug.cgi?id=783835	A-GNO-LIBRS--010817/103
Graphicsmagick					
Graphicsmagick					
NA	17-07-2017	6.8	The ReadMNGImage function in coders/png.c in GraphicsMagick 1.3.26 has an out-of-order CloseBlob call, resulting in a use-after-free via a crafted file. **CVE ID: CVE-2017-11403**	NA	A-GRA-GRAPH--010817/104
NA	26-07-2017	6.8	GraphicsMagick 1.3.26 has a NULL pointer dereference in the WriteMAPImage() function in coders/map.c when processing a non-	http://hg.code.sf.net/p/graphicsmagick/code/r	A-GRA-GRAPH--010817/105

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

			colormapped image, a different vulnerability than CVE-2017-11638. **CVE ID: CVE-2017-11642**	ev/295506 06d8b9	
NA	26-07-2017	6.8	GraphicsMagick 1.3.26 has a segmentation violation in the WriteMAPImage() function in coders/map.c when processing a non-colormapped image, a different vulnerability than CVE-2017-11642. **CVE ID: CVE-2017-11638**	http://hg.code.sf.net/p/graphicsmagick/code/rev/295506 06d8b9	A-GRA-GRAPH--010817/106
Overflow	26-07-2017	7.5	GraphicsMagick 1.3.26 has a heap overflow in the WriteCMYKImage() function in coders/cmyk.c when processing multiple frames that have non-identical widths. **CVE ID: CVE-2017-11643**	http://hg.code.sf.net/p/graphicsmagick/code/rev/d00b74 315a71	A-GRA-GRAPH--010817/107
Overflow	26-07-2017	7.5	GraphicsMagick 1.3.26 has a Memory Leak in the PersistCache function in magick/pixel_cache.c during writing of Magick Persistent Cache (MPC) files. **CVE ID: CVE-2017-11641**	http://hg.code.sf.net/p/graphicsmagick/code/rev/db732abd9318	A-GRA-GRAPH--010817/108
NA	26-07-2017	7.5	GraphicsMagick 1.3.26 has a NULL pointer dereference in the WritePCLImage() function in coders/pcl.c during writes of monochrome images. **CVE ID: CVE-2017-11637**	http://hg.code.sf.net/p/graphicsmagick/code/rev/f3ffc554 1257	A-GRA-GRAPH--010817/109
Overflow	26-07-2017	7.5	GraphicsMagick 1.3.26 has a heap overflow in the WriteRGBImage() function in coders/rgb.c when processing multiple frames that have non-identical widths. **CVE ID: CVE-2017-11636**	http://hg.code.sf.net/p/graphicsmagick/code/rev/39961adf974c	A-GRA-GRAPH--010817/110
Hammock					
Assetview					
Execute Code; SQL Injection	17-07-2017	6.5	SQL injection vulnerability in the AssetView for MacOS Ver.9.2.0 and earlier versions allows remote attackers to execute arbitrary SQL commands via "File Transfer Web Service". **CVE ID: CVE-2017-2241**	https://www.hammock.jp/assetview/info/170714.html	A-HAM-ASSET--010817/111
Hibara					
Attachecase					
Gain Privileges	17-07-2017	9.3	Untrusted search path vulnerability in Self-extracting encrypted files created	https://jvn.jp/en/jp/JV	A-HIB-ATTAC--

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

			by AttacheCase ver.3.2.2.6 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2272**	N61502349/index.html	010817/112
Gain Privileges	17-07-2017	9.3	Untrusted search path vulnerability in Self-extracting encrypted files created by AttacheCase ver.2.8.3.0 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2271**	https://jvn.jp/en/jp/JVN61502349/index.html	A-HIB-ATTAC--010817/113
IBM					
Bigfix Platform					
NA	19-07-2017	5	IBM Tivoli Endpoint Manager uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 123903. **CVE ID: CVE-2017-1224**	http://www.ibm.com/support/docview.wss?uid=swg22005246	A-IBM-BIGFI--010817/114
NA	19-07-2017	5.5	IBM Tivoli Endpoint Manager 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: 123859. **CVE ID: CVE-2017-1219**	http://www.ibm.com/support/docview.wss?uid=swg22006014	A-IBM-BIGFI--010817/115
Gain Information	19-07-2017	5.8	IBM Tivoli Endpoint Manager could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 123902. **CVE ID: CVE-2017-1223**	http://www.ibm.com/support/docview.wss?uid=swg22005246	A-IBM-BIGFI--010817/116
CSRF	19-07-2017	6.8	IBM Tivoli Endpoint Manager is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized	http://www.ibm.com/support/docview.wss?u	A-IBM-BIGFI--010817/117

			actions transmitted from a user that the website trusts. IBM X-Force ID: 123858. **CVE ID: CVE-2017-1218**	id=swg22005246	
Mq Appliance					
Execute Code	18-07-2017	9	IBM MQ Appliance 8.0 and 9.0 could allow an authenticated messaging administrator to execute arbitrary commands on the system, caused by command execution. IBM X-Force ID: 125730. **CVE ID: CVE-2017-1318**	http://www.ibm.com/support/docview.wss?uid=swg22003815	A-IBM-MQ AP--010817/118
Security Guardium					
NA	21-07-2017	5	IBM Security Guardium 10.0 and 10.1 processes patches, image backups and other updates without sufficiently verifying the origin and integrity of the code. IBM X-Force ID: 124742. **CVE ID: CVE-2017-1267**	http://www.ibm.com/support/docview.wss?uid=swg22004424	A-IBM-SECUR--010817/119
Tivoli Monitoring					
Sql	17-07-2017	5.4	IBM Tivoli Monitoring Portal v6 could allow a local (network adjacent) attacker to modify SQL commands to the Portal Server, when default client-server communications, HTTP, are being used. IBM X-Force ID: 123494. **CVE ID: CVE-2017-1183**	http://www.ibm.com/support/docview.wss?uid=swg22003402	A-IBM-TIVOL--010817/120
Execute Code	17-07-2017	5.4	IBM Tivoli Monitoring Portal v6 could allow a local (network adjacent) attacker to execute arbitrary commands on the system, when default client-server default communications, HTTP, are being used. IBM X-Force ID: 123493. **CVE ID: CVE-2017-1182**	http://www.ibm.com/support/docview.wss?uid=swg22003402	A-IBM-TIVOL--010817/121
Tririga Application Platform					
NA	21-07-2017	6.5	Reports executed in the IBM TRIRIGA Application Platform 3.3, 3.4, and 3.5 contains a vulnerability that could allow an authenticated user to execute a report they do not have access to. IBM X-Force ID: 126866. **CVE ID: CVE-2017-1373**	http://www.ibm.com/support/docview.wss?uid=swg22004677	A-IBM-TRIRI--010817/122
NA	21-07-2017	6.5	Builder tools running in the IBM TRIRIGA Application Platform 3.3, 3.4, and 3.5 contains a vulnerability that could allow an authenticated user to execute Builder tool actions they do not	http://www.ibm.com/support/docview.wss?uid=swg2200	A-IBM-TRIRI--010817/123

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

			have access to. IBM X-Force ID: 126864. **CVE ID: CVE-2017-1371**	4674	
Idera					
Uptime Infrastructure Monitor					
Directory Traversal	20-07-2017	5	get2post.php in IDERA Uptime Monitor 7.8 has directory traversal in the file_name parameter. **CVE ID: CVE-2017-11469**	https://blogs.securiteam.com/index.php/archives/3223#more-3223	A-IDE-UPTIM--010817/124
Sql	20-07-2017	7.5	IDERA Uptime Monitor 7.8 has SQL injection in /gadgets/definitions/uptime.CapacityWhatIfGadget/getmetrics.php via the element parameter. **CVE ID: CVE-2017-11471**	https://blogs.securiteam.com/index.php/archives/3223#more-3223	A-IDE-UPTIM--010817/125
Sql	20-07-2017	7.5	IDERA Uptime Monitor 7.8 has SQL injection in /gadgets/definitions/uptime.CapacityWhatifGadget/getxenmetrics.php via the element parameter. **CVE ID: CVE-2017-11470**	https://blogs.securiteam.com/index.php/archives/3223#more-3223	A-IDE-UPTIM--010817/126
Imagemagick					
Imagemagick					
DoS	19-07-2017	6.8	coders/jpeg.c in ImageMagick before 7.0.6-1 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via JPEG data that is too short. **CVE ID: CVE-2017-11450**	https://security-tracker.debian.org/tracker/CVE-2017-11450	A-IMA-IMAGE--010817/127
DoS	19-07-2017	6.8	coders/mpc.c in ImageMagick before 7.0.6-1 does not enable seekable streams and thus cannot validate blob sizes, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an image received from stdin. **CVE ID: CVE-2017-11449**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=867896	A-IMA-IMAGE--010817/128
NA	19-07-2017	7.1	The ReadPESImage function in coders\pes.c in ImageMagick 7.0.6-1 has an infinite loop vulnerability that can cause CPU exhaustion via a crafted PES file. **CVE ID: CVE-2017-11446**	https://github.com/ImageMagick/ImageMagick/issues/537	A-IMA-IMAGE--010817/129

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

DoS	20-07-2017	7.1	The ReadOneDJVUImage function in coders/djvu.c in ImageMagick through 6.9.9-0 and 7.x through 7.0.6-1 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a malformed DJVU image. **CVE ID: CVE-2017-11478**	https://github.com/ImageMagick/ImageMagick/issues/528	A-IMA-IMAGE--010817/130
DoS	21-07-2017	7.1	The ReadOneJNGImage function in coders/png.c in ImageMagick through 6.9.9-0 and 7.x through 7.0.6-1 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a malformed JNG file. **CVE ID: CVE-2017-11505**	https://github.com/ImageMagick/ImageMagick/issues/526	A-IMA-IMAGE--010817/131
DoS	22-07-2017	7.1	The ReadEPTImage function in coders/ept.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (memory consumption) via a crafted file. **CVE ID: CVE-2017-11530**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=867821	A-IMA-IMAGE--010817/132
DoS	22-07-2017	7.1	The ReadDPXImage function in coders/dpx.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (memory consumption) via a crafted file. **CVE ID: CVE-2017-11527**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=867812	A-IMA-IMAGE--010817/133
DoS	22-07-2017	7.1	The ReadOneMNGImage function in coders/png.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a crafted file. **CVE ID: CVE-2017-11526**	https://github.com/ImageMagick/ImageMagick/issues/527	A-IMA-IMAGE--010817/134
DoS	22-07-2017	7.1	The ReadCINImage function in coders/cin.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (memory consumption) via a crafted file. **CVE ID: CVE-2017-11525**	https://github.com/ImageMagick/ImageMagick/issues/519	A-IMA-IMAGE--010817/135
DoS	22-07-2017	7.1	The ReadTXTImage function in coders/txt.c in ImageMagick through 6.9.9-0 and 7.x through 7.0.6-1 allows remote attackers to cause a denial of	https://github.com/ImageMagick/ImageMagick	A-IMA-IMAGE--010817/136

			service (infinite loop) via a crafted file, because the end-of-file condition is not considered. **CVE ID: CVE-2017-11523**	k/issues/591	
DoS	25-07-2017	7.8	Memory leak in AcquireVirtualMemory in ImageMagick before 7 allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors. **CVE ID: CVE-2016-7539**	https://github.com/ImageMagick/ImageMagick/commit/4e81ce8b07219c69a9aeccb0f7f7b927ca6db74c	A-IMA-IMAGE--010817/137
Inmarsat					
Amosconnect 8					
Sql	22-07-2017	5	Blind SQL injection in Inmarsat AmosConnect 8 login form allows remote attackers to access user credentials, including user names and passwords. **CVE ID: CVE-2017-3221**	NA	A-INM-AMOSC--010817/138
Execute Code; Gain Privileges	22-07-2017	10	Hard-coded credentials in AmosConnect 8 allow remote attackers to gain full administrative privileges, including the ability to execute commands on the Microsoft Windows host platform with SYSTEM privileges by abusing AmosConnect Task Manager. **CVE ID: CVE-2017-3222**	NA	A-INM-AMOSC--010817/139
Intelliants					
Subrion Cms					
Sql	19-07-2017	7.5	Subrion CMS before 4.1.6 has a SQL injection vulnerability in /front/actions.php via the $_POST array. **CVE ID: CVE-2017-11445**	https://github.com/intelliants/subrion/issues/480	A-INT-SUBRI--010817/140
Sql	19-07-2017	7.5	Subrion CMS before 4.1.5.10 has a SQL injection vulnerability in /front/search.php via the $_GET array. **CVE ID: CVE-2017-11444**	https://github.com/intelliants/subrion/issues/479	A-INT-SUBRI--010817/141
Jasper Project					
Jasper					
NA	17-07-2017	5	JasPer 2.0.12 is vulnerable to a NULL pointer exception in the function jp2_encode which failed to check to see	NA	A-JAS-JASPE--010817/

			if the image contained at least one component resulting in a denial-of-service. **CVE ID: CVE-2017-1000050**		142
Jenkins					
Jenkins					
Gain Information	17-07-2017	5	The re-key admin monitor was introduced in Jenkins 1.498 and re-encrypted all secrets in JENKINS_HOME with a new key. It also created a backup directory with all old secrets, and the key used to encrypt them. These backups were world-readable and not removed afterwards. Jenkins now deletes the backup directory, if present. Upgrading from before 1.498 will no longer create a backup directory. Administrators relying on file access permissions in their manually created backups are advised to check them for the directory $JENKINS_HOME/jenkins.security.ReKeySecretAdminMonitor/backups, and delete it if present. **CVE ID: CVE-2017-1000362**	https://jenkins.io/security/advisory/2017-02-01/	A-JEN-JENKI--010817/143
Joomla					
Joomla!					
Gain Information	17-07-2017	5	Improper cache invalidation in Joomla! CMS 1.7.3 through 3.7.2 leads to disclosure of form contents. **CVE ID: CVE-2017-9933**	https://developer.joomla.org/security-centre/696-20170601-core-information-disclosure	A-JOO-JOOML--010817/144
Kaspersky					
Anti-virus For Linux Server					
Gain Information	17-07-2017	5	The reportId parameter of the getReportStatus action method can be abused in the web interface in Kaspersky Anti-Virus for Linux File Server before Maintenance Pack 2 Critical Fix 4 (version 8.0.4.312) to read arbitrary files with kluser privileges. **CVE ID: CVE-2017-9812**	NA	A-KAS-ANTI---010817/145

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

CSRF	17-07-2017	6.8	There are no Anti-CSRF tokens in any forms on the web interface in Kaspersky Anti-Virus for Linux File Server before Maintenance Pack 2 Critical Fix 4 (version 8.0.4.312). This would allow an attacker to submit authenticated requests when an authenticated user browses an attacker-controlled domain. **CVE ID: CVE-2017-9810**	NA	A-KAS-ANTI---010817/146
NA	17-07-2017	10	The kluser is able to interact with the kav4fs-control binary in Kaspersky Anti-Virus for Linux File Server before Maintenance Pack 2 Critical Fix 4 (version 8.0.4.312). By abusing the quarantine read and write operations, it is possible to elevate the privileges to root. **CVE ID: CVE-2017-9811**	NA	A-KAS-ANTI---010817/147
Keepass					
Keepass					
Gain Information	17-07-2017	5	The entry details view function in KeePass version 1.32 inadvertently decrypts certain database entries into memory, which may result in the disclosure of sensitive information. **CVE ID: CVE-2017-1000066**	http://keepass.info/news/news_all.html	A-KEE-KEEPA--010817/148
Kitto Project					
Kitto					
NA	17-07-2017	5	kittoframework kitto version 0.5.1 is vulnerable to memory exhaustion in the router resulting in DoS. **CVE ID: CVE-2017-1000064**	https://elixirforum.com/t/kitto-a-framework-for-interactive-dashboards/2089/13	A-KIT-KITTO--010817/149
Execute Code; Directory Traversal	17-07-2017	5	kittoframework kitto 0.5.1 is vulnerable to directory traversal in the router resulting in remote code execution **CVE ID: CVE-2017-1000062**	https://elixirforum.com/t/kitto-a-framework-for-interactive-dashboards/2089/13	A-KIT-KITTO--010817/150
Koozali					
Sme Server					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

NA	17-07-2017	5.8	Koozali Foundation SME Server versions 8.x, 9.x, 10.x are vulnerable to an open URL redirect vulnerability in the user web login function resulting in unauthorized account access. **CVE ID: CVE-2017-1000027**	NA	A-KOO-SME S--010817/151
Libexpat Project					
Libexpat					
NA	25-07-2017	5	XML External Entity vulnerability in libexpat 2.2.0 and earlier (Expat XML Parser Library) allows attackers to put the parser in an infinite loop using a malformed external entity definition from an external DTD. **CVE ID: CVE-2017-9233**	https://github.com/libexpat/libexpat/blob/master/expat/Changes	A-LIB-LIBEX--010817/152
Libinfinity Project					
Libinfinity					
NA	21-07-2017	7.5	libinfinity before 0.6.6-1 does not validate expired SSL certificates, which allows remote attackers to have unspecified impact via unknown vectors. **CVE ID: CVE-2015-3886**	https://bugzilla.redhat.com/show_bug.cgi?id=1221266	A-LIB-LIBIN--010817/153
Libsass					
Libsass					
DoS	17-07-2017	5	There is an illegal address access in ast.cpp of LibSass 3.4.5. A crafted input will lead to a remote denial of service attack. **CVE ID: CVE-2017-11342**	https://bugzilla.redhat.com/show_bug.cgi?id=1470722	A-LIB-LIBSA--010817/154
Denial of Service; Overflow	17-07-2017	5	There is a heap based buffer over-read in lexer.hpp of LibSass 3.4.5. A crafted input will lead to a remote denial of service attack. **CVE ID: CVE-2017-11341**	https://bugzilla.redhat.com/show_bug.cgi?id=1470714	A-LIB-LIBSA--010817/155
DoS	22-07-2017	5	There is a stack consumption vulnerability in the Parser::advanceToNextToken function in parser.cpp in LibSass 3.4.5. A crafted input may lead to remote denial of service. **CVE ID: CVE-2017-11556**	https://bugzilla.redhat.com/show_bug.cgi?id=1471786	A-LIB-LIBSA--010817/156
DoS	22-07-2017	5	There is an illegal address access in the Eval::operator function in eval.cpp in LibSass 3.4.5. A crafted input will lead to a remote denial of service. **CVE ID: CVE-2017-11555**	https://bugzilla.redhat.com/show_bug.cgi?id=1471782	A-LIB-LIBSA--010817/157

DoS	22-07-2017	5	There is a stack consumption vulnerability in the lex function in parser.hpp (as used in sassc) in LibSass 3.4.5. A crafted input will lead to a remote denial of service. **CVE ID: CVE-2017-11554**	NA	A-LIB-LIBSA--010817/158
Libtiff					
Libtiff					
Denial of Service; Execute Code; Overflow	17-07-2017	6.8	There is a heap based buffer overflow in tools/tiff2pdf.c of LibTIFF 4.0.8 via a PlanarConfig=Contig image, which causes a more than one hundred bytes out-of-bounds write (related to the ZIPDecode function in tif_zip.c). A crafted input may lead to a remote denial of service attack or an arbitrary code execution attack. **CVE ID: CVE-2017-11335**	http://bugzilla.maptools.org/show_bug.cgi?id=2715	A-LIB-LIBTI--010817/159
Logicaldoc					
Logicaldoc					
NA	17-07-2017	7.5	LogicalDoc CommunityEdition 7.5.3 and prior contain an Incorrect access control which could leave to privilege escalation **CVE ID: CVE-2017-1000022**	http://blog.logicaldoc.com/	A-LOG-LOGIC--010817/160
NA	17-07-2017	7.5	LogicalDoc CommunityEdition 7.5.3 and prior is vulnerable to XXE when indexing XML documents. **CVE ID: CVE-2017-1000021**	http://blog.logicaldoc.com/	A-LOG-LOGIC--010817/161
Mautic					
Mautic					
NA	17-07-2017	5	Mautic 2.6.1 and earlier fails to set flags on session cookies. **CVE ID: CVE-2017-1000046**	https://www.trustmatta.com/advisories/MATTA-2017-002.txt	A-MAU-MAUTI--010817/162
Bypass; CSRF	17-07-2017	6.8	Mautic SSO/OAuth2 plugins are vulnerable to CSRF of the state parameter resulting in authentication bypass through clickjacking. **CVE ID: CVE-2017-1000045**	https://www.trustmatta.com/advisories/MATTA-2017-001.txt	A-MAU-MAUTI--010817/163
Mediawiki					
Mediawiki					
NA	25-07-2017	5	The MWOAuthDataStore::lookup_token function in Extension:OAuth for	https://phabricator.wik	A-MED-MEDIA--

			MediaWiki 1.25.x before 1.25.3, 1.24.x before 1.24.4, and before 1.23.11 does not properly validate the signature when checking the authorization signature, which allows remote registered Consumers to use another Consumer's credentials by leveraging knowledge of the credentials. **CVE ID: CVE-2015-8009**	imedia.org/T103023	010817/164
Metinfo Project					
Metinfo					
Directory Traversal	20-07-2017	5	A directory traversal vulnerability exists in MetInfo 5.3.17. A remote attacker can use ..\ to delete any .zip file via the filenames parameter to /admin/system/database/filedown.php. **CVE ID: CVE-2017-11500**	http://blackwolfsec.cc/2017/07/20/Metinfo-directory-traversal-bypass/	A-MET-METIN--010817/165
Microsec					
E-szigno					
NA	21-07-2017	6.8	Microsec e-Szigno before 3.2.7.12 allows remote attackers to perform XML signature wrapping attacks via an e-akta signed document with a ds:Object node with a crafted payload prepended to a valid ds:Object. **CVE ID: CVE-2015-3931**	NA	A-MIC-E-SZI--010817/166
Microsoft					
Edge					
Execute Code; Overflow; Memory Corruption	17-07-2017	9.3	A remote code execution vulnerability exists in the way affected Microsoft scripting engine render when handling objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user, aka "Scripting Engine Memory Corruption Vulnerability." **CVE ID: CVE-2017-0152**	https://github.com/Microsoft/ChakraCore/commit/9da019424601325a6e95e6be0fa03d7d21d0b517	A-MIC-EDGE--010817/167
Modx					
Revolution					
Sql	17-07-2017	6.5	MODX Revolution version 2.x - 2.5.6 is	https://gith	A-MOD-

			vulnerable to blind SQL injection caused by improper sanitization by the escape method resulting in authenticated user accessing database and possibly escalating privileges. **CVE ID: CVE-2017-1000067**	ub.com/modxcms/revolution/blob/9bf1c6cf7bdc12190b404f93ce7798b39c07bc59/core/xpdo/changelog.txt	REVOL--010817/168
Nancyfx					
Nancy					
Execute Code; Cross Site Request Forgery	20-07-2017	7.5	Csrf.cs in NancyFX Nancy before 1.4.4 and 2.x before 2.0-dangermouse has Remote Code Execution via Deserialization of JSON data in a CSRF Cookie. **CVE ID: CVE-2017-9785**	https://github.com/NancyFx/Nancy/releases/tag/v1.4.4	A-NAN-NANCY--010817/169
Netlock					
Mokka					
NA	21-07-2017	6.8	Netlock Mokka before 2.7.8.1204 allows remote attackers to perform XML signature wrapping attacks via an e-akta signed document with a ds:Object node with a crafted payload prepended to a valid ds:Object. **CVE ID: CVE-2015-3932**	NA	A-NET-MOKKA--010817/170
Nodejs					
Node.js					
NA	25-07-2017	5	Node.js v4.0 through v4.8.3, all versions of v5.x, v6.0 through v6.11.0, v7.0 through v7.10.0, and v8.0 through v8.1.3 was susceptible to hash flooding remote DoS attacks as the HashTable seed was constant across a given released version of Node.js. This was a result of building with V8 snapshots enabled by default which caused the initially randomized seed to be overwritten on startup. **CVE ID: CVE-2017-11499**	https://nodejs.org/en/blog/vulnerability/july-2017-security-releases/	A-NOD-NODE.--010817/171
Nss Compat Ossl Project					
Nss Compat Ossl					
NA	25-07-2017	7.5	The cipherstring parsing code in nss_compat_ossl while in multi-keyword mode does not match the expected set of ciphers for a given cipher combination,	https://bugzilla.redhat.com/show_bug.cgi?id=	A-NSS-NSS C--010817/172

			which allows attackers to have unspecified impact via unknown vectors. **CVE ID: CVE-2015-3278**	1238326	
NTP					
NTP					
NA	24-07-2017	5.8	The "pidfile" or "driftfile" directives in NTP ntpd 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77, when ntpd is configured to allow remote configuration, allows remote attackers with an IP address that is allowed to send configuration requests, and with knowledge of the remote configuration password to write to arbitrary files via the :config command. **CVE ID: CVE-2015-7703**	https://bugzilla.redhat.com/show_bug.cgi?id=1254547	A-NTP-NTP--010817/173
Oauth2 Proxy Project					
Oauth2 Proxy					
NA	17-07-2017	5.8	The Bitly oauth2_proxy in version 2.1 and earlier was affected by an open redirect vulnerability during the start and termination of the 2-legged OAuth flow. This issue was caused by improper input validation and a violation of RFC-6819 **CVE ID: CVE-2017-1000070**	https://github.com/bitly/oauth2_proxy/pull/359	A-OAU-OAUTH--010817/174
CSRF	17-07-2017	6.8	CSRF in Bitly oauth2_proxy 2.1 during authentication flow **CVE ID: CVE-2017-1000069**	https://github.com/bitly/oauth2_proxy/pull/360	A-OAU-OAUTH--010817/175
Openmpt					
Libopenmpt; Openmpt					
Execute Code; Overflow	17-07-2017	6.8	soundlib/Load_psm.cpp in OpenMPT through 1.26.12.00 and libopenmpt before 0.2.8461-beta26 has a heap buffer overflow with the potential for arbitrary code execution via a crafted PSM File that triggers use of the same sample slot for two samples. **CVE ID: CVE-2017-11311**	https://source.openmpt.org/browse/openmpt/trunk/?rev=6800	A-OPE-LIBOP--010817/176
Oracle					
Glassfish Server					
NA	17-07-2017	5	Oracle, GlassFish Server Open Source Edition 3.0.1 (build 22) is vulnerable to Java Key Store Password Disclosure	https://www.trustwave.com/Reso	A-ORA-GLASS--010817/

			vulnerability that makes it possible to provide an unauthenticated attacker plain text password of administrative user and grant access to the web-based administration interface. **CVE ID: CVE-2017-1000030**	urces/Security-Advisories/Advisories/TWSL2016-011/?fid=8037	177
Gain Information; File Inclusion	17-07-2017	5	Oracle, GlassFish Server Open Source Edition 3.0.1 (build 22) is vulnerable to Local File Inclusion vulnerability that makes it possible to include arbitrary files on the server, this vulnerability can be exploited without any prior authentication. **CVE ID: CVE-2017-1000029**	https://www.trustwave.com/Resources/Security-Advisories/Advisories/TWSL2016-011/?fid=8037	A-ORA-GLASS--010817/178
Directory Traversal	17-07-2017	5	Oracle, GlassFish Server Open Source Edition 4.1 is vulnerable to both authenticated and unauthenticated Directory Traversal vulnerability that can be exploited by issuing a specially crafted HTTP GET request. **CVE ID: CVE-2017-1000028**	https://www.trustwave.com/Resources/Security-Advisories/Advisories/TWSL2015-016/?fid=6904	A-ORA-GLASS--010817/179
Orientdb					
Orientdb					
Execute Code	19-07-2017	10	OrientDB through 2.2.22 does not enforce privilege requirements during "where" or "fetchplan" or "order by" use, which allows remote attackers to execute arbitrary OS commands via a crafted request. **CVE ID: CVE-2017-11467**	NA	A-ORI-ORIEN--010817/180
Panda Security					
Panda Antivirus Pro 2015; Panda Global Protection 2015; Panda Gold Protection 2015; Panda Internet Security 2015					
Execute Code; Overflow	25-07-2017	7.2	Heap-based buffer overflow in Panda Security Kernel Memory Access Driver 1.0.0.13 allows attackers to execute arbitrary code with kernel privileges via a crafted size input for allocated kernel paged pool and allocated non-paged pool buffers. **CVE ID: CVE-2015-1438**	NA	A-PAN-PANDA--010817/181

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

PHP					
PHP					
Denial of Service; Overflow	17-07-2017	7.5	In PHP 7.x before 7.0.21 and 7.1.x before 7.1.7, ext/intl/msgformat/msgformat_parse.c does not restrict the locale length, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact within International Components for Unicode (ICU) for C/C++ via a long first argument to the msgfmt_parse_message function. **CVE ID: CVE-2017-11362**	https://bugs.php.net/bug.php?id=73473	A-PHP-PHP--010817/182
Phpmyadmin					
Phpmyadmin					
NA	17-07-2017	5	phpMyAdmin 4.0, 4.4., and 4.6 are vulnerable to a DOS attack in the replication status by using a specially crafted table name **CVE ID: CVE-2017-1000018**	https://www.phpmyadmin.net/security/PMASA-2017-7	A-PHP-PHPMY--010817/183
NA	17-07-2017	5	A weakness was discovered where an attacker can inject arbitrary values in to the browser cookies. This is a re-issue of an incomplete fix from PMASA-2016-18. **CVE ID: CVE-2017-1000016**	https://www.phpmyadmin.net/security/PMASA-2017-5	A-PHP-PHPMY--010817/184
NA	17-07-2017	5	phpMyAdmin 4.0, 4.4, and 4.6 are vulnerable to a DOS weakness in the table editing functionality **CVE ID: CVE-2017-1000014**	https://www.phpmyadmin.net/security/PMASA-2017-3	A-PHP-PHPMY--010817/185
NA	17-07-2017	5.8	phpMyAdmin 4.0, 4.4, and 4.6 are vulnerable to an open redirect weakness **CVE ID: CVE-2017-1000013**	https://www.phpmyadmin.net/security/PMASA-2017-1	A-PHP-PHPMY--010817/186
NA	17-07-2017	6.5	phpMyAdmin 4.0, 4.4 and 4.6 are vulnerable to a weakness where a user with appropriate permissions is able to connect to an arbitrary MySQL server **CVE ID: CVE-2017-1000017**	https://www.phpmyadmin.net/security/PMASA-2017-6	A-PHP-PHPMY--010817/187
Phpmybackuppro					
Phpmybackuppro					
NA	21-07-2017	6	phpMyBackupPro 2.5 and earlier does not properly escape the "." character in request parameters, which allows	NA	A-PHP-PHPMY--010817/

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

			remote authenticated users with knowledge of a web-accessible and web-writeable directory on the target system to inject and execute arbitrary PHP scripts by injecting scripts via the path, filename, and dirs parameters to scheduled.php, and making requests to injected scripts. **CVE ID: CVE-2015-3640**		188
Execute Code	21-07-2017	6.5	phpMyBackupPro 2.5 and earlier does not properly sanitize input strings, which allows remote authenticated users to execute arbitrary PHP code by storing a crafted string in a user configuration file. **CVE ID: CVE-2015-3639**	NA	A-PHP-PHPMY--010817/189
Execute Code	21-07-2017	6.5	phpMyBackupPro before 2.5 does not validate integer input, which allows remote authenticated users to execute arbitrary PHP code by injecting scripts via the path, filename, and period parameters to scheduled.php, and making requests to injected scripts, or by injecting PHP into a PHP configuration variable via a PHP variable variable. **CVE ID: CVE-2015-3638**	NA	A-PHP-PHPMY--010817/190
Project-redcap					
Redcap					
CSRF	18-07-2017	6.8	REDCap before 7.5.1 has CSRF in the deletion feature of the File Repository and File Upload components. **CVE ID: CVE-2017-10961**	NA	A-PRO-REDCA--010817/191
Rbenv					
Rbenv					
Execute Code; Directory Traversal	17-07-2017	7.5	rbenv (all current versions) is vulnerable to Directory Traversal in the specification of Ruby version resulting in arbitrary code execution **CVE ID: CVE-2017-1000047**	https://github.com/justinsteven/advisories/blob/master/2017_rbenv_ruby_version_directory_traversal.md	A-RBE-RBENV--010817/192
Resume-next					
Filecapsule Deluxe Portable					
Gain	17-07-2017	9.3	Untrusted search path vulnerability in	http://resu	A-RES-

Privileges			Encrypted files in self-decryption format created by FileCapsule Deluxe Portable Ver.2.0.9 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2270**	menext.blog.fc2.com/blog-entry-30.html	FILEC--010817/193
Gain Privileges	17-07-2017	9.3	Untrusted search path vulnerability in FileCapsule Deluxe Portable Ver.2.0.9 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2269**	http://resumenext.blog.fc2.com/blog-entry-30.html	A-RES-FILEC--010817/194
Gain Privileges	17-07-2017	9.3	Untrusted search path vulnerability in Encrypted files in self-decryption format created by FileCapsule Deluxe Portable Ver.1.0.5.1 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2268**	http://resumenext.blog.fc2.com/blog-entry-30.html	A-RES-FILEC--010817/195
Gain Privileges	17-07-2017	9.3	Untrusted search path vulnerability in FileCapsule Deluxe Portable Ver.1.0.5.1 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2267**	http://resumenext.blog.fc2.com/blog-entry-30.html	A-RES-FILEC--010817/196
Gain Privileges	17-07-2017	9.3	Untrusted search path vulnerability in Encrypted files in self-decryption format created by FileCapsule Deluxe Portable Ver.1.0.4.1 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2266**	http://resumenext.blog.fc2.com/blog-entry-30.html	A-RES-FILEC--010817/197
Gain Privileges	17-07-2017	9.3	Untrusted search path vulnerability in FileCapsule Deluxe Portable Ver.1.0.4.1 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2265**	http://resumenext.blog.fc2.com/blog-entry-30.html	A-RES-FILEC--010817/198
Rootkit Hunter Project					
Rkhunter					
Execute Code	21-07-2017	7.5	rkhunter versions before 1.4.4 are vulnerable to file download over insecure channel when doing mirror update resulting into potential remote code execution. **CVE ID: CVE-2017-7480**	http://seclists.org/oss-sec/2017/q2/643	A-ROO-RKHUN--010817/199
Ruby-lang					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

Ruby					
DoS; Bypass	19-07-2017	7.5	The parser_yyerror function in the UTF-8 parser in Ruby 2.4.1 allows attackers to cause a denial of service (invalid write or read) or possibly have unspecified other impact via a crafted Ruby script, related to the parser_tokadd_utf8 function in parse.y. NOTE: this might have security relevance as a bypass of a $SAFE protection mechanism. **CVE ID: CVE-2017-11465**	NA	A-RUB-RUBY--010817/200
SAP					
Trex					
Execute Code	25-07-2017	7.5	SAP TREX 7.10 allows remote attackers to (1) read arbitrary files via an fget command or (2) write to arbitrary files and consequently execute arbitrary code via an fdir command, aka SAP Security Note 2419592. **CVE ID: CVE-2017-11459**	https://erpscan.com/advisories/erpscan-17-019-sap-trex-rce/	A-SAP-TREX--010817/201
Sipcrack					
Sipcrack					
Overflow	26-07-2017	5	A memory leak was found in the way SIPcrack 0.2 handled processing of SIP traffic, because a lines array was mismanaged. A remote attacker could potentially use this flaw to crash long-running sipdump network sniffing sessions. **CVE ID: CVE-2017-11655**	http://openwall.com/lists/oss-security/2017/07/26/1	A-SIP-SIPCR--010817/202
Sourcenext					
File Compact					
Gain Privileges	17-07-2017	9.3	Untrusted search path vulnerability in Self-extracting archive files created by File Compact Ver.5 version 5.09 and earlier, Ver.6 version 6.01 and earlier, Ver.7 version 7.01 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2252**	https://jvn.jp/en/jp/JVN29939155/index.html	A-SOU-FILE --010817/203
Subsonic					
Subsonic					
CSRF	21-07-2017	5.1	Cross-site request forgery (CSRF) vulnerability in subsonic 6.1.1 allows remote attackers with knowledge of the target username to hijack the	https://www.exploit-db.com/exploits/42117	A-SUB-SUBSO--010817/204

			authentication of users for requests that change passwords via a crafted request to userSettings.view. **CVE ID: CVE-2017-9415**	/	
CSRF	25-07-2017	6.8	Multiple cross-site request forgery (CSRF) vulnerabilities in the Podcast feature in Subsonic 6.1.1 allow remote attackers to hijack the authentication of users for requests that (1) subscribe to a podcast via the add parameter to podcastReceiverAdmin.view or (2) update Internet Radio Settings via the urlRedirectCustomUrl parameter to networkSettings.view. NOTE: These vulnerabilities can be exploited to conduct server-side request forgery (SSRF) attacks. **CVE ID: CVE-2017-9413**	NA	A-SUB-SUBSO--010817/205
Tcpdump					
Tcpdump					
NA	22-07-2017	5	tcpdump 4.9.0 has a Segmentation Violation in the compressed_sl_print function in print-sl.c:253:34. **CVE ID: CVE-2017-11545**	NA	A-TCP-TCPDU--010817/206
NA	22-07-2017	5	tcpdump 4.9.0 has a Segmentation Violation in the compressed_sl_print function in print-sl.c:229:3. **CVE ID: CVE-2017-11544**	NA	A-TCP-TCPDU--010817/207
Overflow	22-07-2017	7.5	tcpdump 4.9.0 has a buffer overflow in the sliplink_print function in print-sl.c. **CVE ID: CVE-2017-11543**	NA	A-TCP-TCPDU--010817/208
Overflow	22-07-2017	7.5	tcpdump 4.9.0 has a heap-based buffer over-read in the pimv1_print function in print-pim.c. **CVE ID: CVE-2017-11542**	NA	A-TCP-TCPDU--010817/209
Overflow	22-07-2017	7.5	tcpdump 4.9.0 has a heap-based buffer over-read in the lldp_print function in print-lldp.c, related to util-print.c. **CVE ID: CVE-2017-11541**	NA	A-TCP-TCPDU--010817/210
Tilde Cms Project					
Tilde Cms					
Bypass	24-07-2017	5	An issue was discovered in Tilde CMS 1.0.1. It is possible to bypass the implemented restrictions on arbitrary file upload via a filename.+php	https://backbox.org/membership/sharing-	A-TIL-TILDE--010817/211

			manipulation. **CVE ID: CVE-2017-11326**	board/tilde-cms-v1-01-multiple-vulnerabilities/	
Gain Information	24-07-2017	5	An issue was discovered in Tilde CMS 1.0.1. Arbitrary files can be read via a file=../ attack on actionphp/download.File.php. **CVE ID: CVE-2017-11325**	https://backbox.org/membership/sharing-board/tilde-cms-v1-01-multiple-vulnerabilities/	A-TIL-TILDE--010817/212
Sql	24-07-2017	7.5	An issue was discovered in Tilde CMS 1.0.1. Due to missing escaping of the backtick character, a SELECT query in class.SystemAction.php is vulnerable to SQL Injection. The vulnerability can be triggered via a POST request to /actionphp/action.input.php with the id parameter. **CVE ID: CVE-2017-11324**	https://backbox.org/membership/sharing-board/tilde-cms-v1-01-multiple-vulnerabilities/	A-TIL-TILDE--010817/213
Wireshark					
Wireshark					
NA	18-07-2017	5	In Wireshark 2.2.0 to 2.2.7 and 2.0.0 to 2.0.13, the AMQP dissector could crash. This was addressed in epan/dissectors/packet-amqp.c by checking for successful list dissection. **CVE ID: CVE-2017-11408**	https://www.wireshark.org/security/wnpa-sec-2017-34.html	A-WIR-WIRES--010817/214
NA	18-07-2017	5	In Wireshark 2.2.0 to 2.2.7 and 2.0.0 to 2.0.13, the MQ dissector could crash. This was addressed in epan/dissectors/packet-mq.c by validating the fragment length before a reassembly attempt. **CVE ID: CVE-2017-11407**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=13792	A-WIR-WIRES--010817/215
NA	18-07-2017	7.8	In Wireshark through 2.0.13 and 2.2.x through 2.2.7, the openSAFETY dissector could crash or exhaust system memory. This was addressed in epan/dissectors/packet-opensafety.c by adding length validation. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-9350. **CVE ID: CVE-2017-11411**	https://www.wireshark.org/security/wnpa-sec-2017-28.html	A-WIR-WIRES--010817/216

NA	18-07-2017	7.8	In Wireshark through 2.0.13 and 2.2.x through 2.2.7, the WBXML dissector could go into an infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-wbxml.c by adding validation of the relationships between indexes and lengths. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-7702. **CVE ID: CVE-2017-11410**	https://www.wireshark.org/security/wnpa-sec-2017-13.html	A-WIR-WIRES--010817/217
NA	18-07-2017	7.8	In Wireshark 2.0.0 to 2.0.13, the GPRS LLC dissector could go into a large loop. This was addressed in epan/dissectors/packet-gprs-llc.c by using a different integer data type. **CVE ID: CVE-2017-11409**	https://www.wireshark.org/security/wnpa-sec-2017-37.html	A-WIR-WIRES--010817/218
NA	18-07-2017	7.8	In Wireshark 2.2.0 to 2.2.7 and 2.0.0 to 2.0.13, the DOCSIS dissector could go into an infinite loop. This was addressed in plugins/docsis/packet-docsis.c by rejecting invalid Frame Control parameter values. **CVE ID: CVE-2017-11406**	https://www.wireshark.org/security/wnpa-sec-2017-36.html	A-WIR-WIRES--010817/219
Yahoo					
Toolbar					
Gain Privileges	17-07-2017	9.3	Untrusted search path vulnerability in Installer of Yahoo! Toolbar (for Internet explorer) v8.0.0.6 and earlier, with its timestamp prior to June 13, 2017, 18:18:55 allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2253**	https://jvn.jp/en/jp/JVN02852421/index.html	A-YAH-TOOLB--010817/220
Zohocorp					
Manageengine Desktop Central					
Execute Code	17-07-2017	7.5	Zoho ManageEngine Desktop Central before build 100092 allows remote attackers to execute arbitrary code via vectors involving the upload of help desk videos. **CVE ID: CVE-2017-11346**	https://www.manageengine.com/products/desktop-central/remote-code-execution.html	A-ZOH-MANAG--010817/221

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

Application; Operating System (A / OS)					
Apple/Apple					
Apple Tv/Iphone Os; Mac Os X					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. tvOS before 10.2.2 is affected. The issue involves the "CoreAudio" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted movie file. **CVE ID: CVE-2017-7008**	https://support.apple.com/HT207923	A-OS-APP-APPLE--010817/222
Apple Tv/Iphone Os;Mac Os X;Watchos					
Denial of Service; Execute Code; Overflow	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. tvOS before 10.2.2 is affected. watchOS before 3.2.3 is affected. The issue involves the "libarchive" component. It allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a crafted archive file. **CVE ID: CVE-2017-7068**	https://support.apple.com/HT207924	A- OS-APP-APPLE--010817/223
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. tvOS before 10.2.2 is affected. watchOS before 3.2.3 is affected. The issue involves the "libxpc" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7047**	https://support.apple.com/HT207922	A- OS-APP-APPLE--010817/224
Denial of Service; Execute Code; Overflow	20-07-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. tvOS before 10.2.2 is affected. watchOS before 3.2.3 is affected. The issue involves the "Contacts" component. A buffer overflow allows remote attackers to execute arbitrary code or cause a denial of service (application crash). **CVE ID: CVE-2017-7062**	https://support.apple.com/HT207925	A- OS-APP-APPLE--010817/225
Denial of	20-07-2017	9.3	An issue was discovered in certain Apple	https://sup	A- OS-

Service; Execute Code; Overflow; Memory Corruption			products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. tvOS before 10.2.2 is affected. watchOS before 3.2.3 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7069**	port.apple.com/HT207925	APP-APPLE--010817/226
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. tvOS before 10.2.2 is affected. watchOS before 3.2.3 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7027**	https://support.apple.com/HT207925	A- OS-APP-APPLE--010817/227
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. tvOS before 10.2.2 is affected. watchOS before 3.2.3 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7026**	https://support.apple.com/HT207925	A- OS-APP-APPLE--010817/228
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. tvOS before 10.2.2 is affected. watchOS before 3.2.3 is affected. The issue involves the "IOUSBFamily" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7009**	https://support.apple.com/HT207925	A- OS-APP-APPLE--010817/229
Apple Tv;Icloud;Itunes/Iphone Os;Mac Os X					
Denial of Service; Gain Information	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected.	https://support.apple.com/HT207928	A- OS-APP-APPLE--010817/230

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

			The issue involves the "libxml2" component. It allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a crafted XML file. **CVE ID: CVE-2017-7010**		
Apple Tv;Icloud;Itunes/Iphone Os;Mac Os X;Watchos					
Denial of Service; Gain Information	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. watchOS before 3.2.3 is affected. The issue involves the "libxml2" component. It allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a crafted XML file. **CVE ID: CVE-2017-7013**	https://support.apple.com/HT207927	A- OS-APP-APPLE--010817/231
Apple Tv;Icloud;Itunes;Safari/Iphone Os					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7048**	https://support.apple.com/HT207927	A- OS-APP-APPLE--010817/232
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7046**	https://support.apple.com/HT207927	A- OS-APP-APPLE--010817/233
Denial of Service;	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected.	https://support.apple.c	A- OS-APP-

Execute Code; Overflow; Memory Corruption			Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7039**	om/HT207928	APPLE--010817/234
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7037**	https://support.apple.com/HT207928	A- OS-APP-APPLE--010817/235
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7034**	https://support.apple.com/HT207927	A- OS-APP-APPLE--010817/236
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7030**	https://support.apple.com/HT207928	A- OS-APP-APPLE--010817/237
Denial of	20-07-2017	6.8	An issue was discovered in certain Apple	https://sup	A- OS-

Service; Execute Code; Overflow; Memory Corruption			products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7020**	port.apple.com/HT207927	APP-APPLE--010817/238
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit Page Loading" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7019**	https://support.apple.com/HT207928	A- OS-APP-APPLE--010817/239
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7018**	https://support.apple.com/HT207928	A- OS-APP-APPLE--010817/240
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	https://support.apple.com/HT207927	A- OS-APP-APPLE--010817/241

			CVE ID: CVE-2017-7061		
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7056**	https://support.apple.com/HT207928	A- OS-APP-APPLE--010817/242
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7055**	https://support.apple.com/HT207927	A- OS-APP-APPLE--010817/243
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7052**	https://support.apple.com/HT207927	A- OS-APP-APPLE--010817/244
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and	https://support.apple.com/HT207928	A- OS-APP-APPLE--010817/245

			application crash) via a crafted web site. **CVE ID: CVE-2017-7049**		
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7042**	https://support.apple.com/HT207928	A- OS-APP-APPLE--010817/246
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7041**	https://support.apple.com/HT207927	A- OS-APP-APPLE--010817/247
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. tvOS before 10.2.2 is affected. watchOS before 3.2.3 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7025**	https://support.apple.com/HT207925	A- OS-APP-APPLE--010817/248
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. tvOS before 10.2.2 is affected. watchOS before 3.2.3 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7024**	https://support.apple.com/HT207925	A- OS-APP-APPLE--010817/249
Denial of	20-07-2017	9.3	An issue was discovered in certain Apple	https://sup	A- OS-

Service; Execute Code; Overflow; Memory Corruption			products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. tvOS before 10.2.2 is affected. watchOS before 3.2.3 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7023**	port.apple.com/HT207924	APP-APPLE--010817/250
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. macOS before 10.12.6 is affected. tvOS before 10.2.2 is affected. watchOS before 3.2.3 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7022**	https://support.apple.com/HT207925	A- OS-APP-APPLE--010817/251
Icloud; Itunes; Safari / Iphone Os					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7043**	https://support.apple.com/HT207927	A- OS-APP-ICLOU--010817/252
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. tvOS before 10.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7040**	https://support.apple.com/HT207927	A- OS-APP-ICLOU--010817/253
Denial of Service; Execute Code;	20-07-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. Safari before 10.1.2 is affected. iCloud	https://support.apple.com/HT207	A- OS-APP-ICLOU--

Overflow; Memory Corruption			before 6.2.2 on Windows is affected. iTunes before 12.6.2 on Windows is affected. The issue involves the "WebKit Web Inspector" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-7012**	927	010817/254
Operating System (OS)					
Airlink101					
Skyipcam1620w Wireless N Mpeg4 3gpp Firmware					
Execute Code	24-07-2017	9	snwrite.cgi in AirLink101 SkyIPCam1620W Wireless N MPEG4 3GPP network camera with firmware FW_AIC1620W_1.1.0-12_20120709_r1192.pck allows remote authenticated users to execute arbitrary OS commands via shell metacharacters in the mac parameter. **CVE ID: CVE-2015-2280**	NA	O-AIR-SKYIP--010817/255
Airlive					
Bu-2015 Firmware;Bu-3026 Firmware;Md-3025 Firmware					
Execute Code	24-07-2017	10	cgi_test.cgi in AirLive BU-2015 with firmware 1.03.18, BU-3026 with firmware 1.43, and MD-3025 with firmware 1.81 allows remote attackers to execute arbitrary OS commands via shell metacharacters after an "&" (ampersand) in the write_mac write_pid, write_msn, write_tan, or write_hdv parameter. **CVE ID: CVE-2015-2279**	NA	O-AIR-BU-20--010817/256
Alpinelinux					
Alpine Linux					
Denial of Service; Execute Code; Overflow	17-07-2017	6.8	A heap overflow in apk (Alpine Linux's package manager) allows a remote attacker to cause a denial of service, or achieve code execution, by crafting a malicious APKINDEX.tar.gz file with a bad pax header block. **CVE ID: CVE-2017-9671**	NA	O-ALP-ALPIN--010817/257
Denial of Service; Execute Code; Overflow	17-07-2017	6.8	A heap overflow in apk (Alpine Linux's package manager) allows a remote attacker to cause a denial of service, or achieve code execution by crafting a malicious APKINDEX.tar.gz file.	NA	O-ALP-ALPIN--010817/258

			CVE ID: CVE-2017-9669		
Apple					
Iphone Os					
DoS	20-07-2017	5	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. The issue involves the "EventKitUI" component. It allows remote attackers to cause a denial of service (resource consumption and application crash). **CVE ID: CVE-2017-7007**	https://support.apple.com/HT207923	O-APP-IPHON--010817/259
Iphone Os;Watchos					
DoS	20-07-2017	5	An issue was discovered in certain Apple products. iOS before 10.3.3 is affected. watchOS before 3.2.3 is affected. The issue involves the "Messages" component. It allows remote attackers to cause a denial of service (memory consumption and application crash). **CVE ID: CVE-2017-7063**	https://support.apple.com/HT207923	O-APP-IPHON--010817/260
Mac Os X					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.12.6 is affected. The issue involves the "afclip" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted audio file. **CVE ID: CVE-2017-7033**	https://support.apple.com/HT207922	O-APP-MAC O--010817/261
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.12.6 is affected. The issue involves the "Foundation" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted file. **CVE ID: CVE-2017-7031**	https://support.apple.com/HT207922	O-APP-MAC O--010817/262
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.12.6 is affected. The issue involves the "afclip" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted audio file. **CVE ID: CVE-2017-7016**	https://support.apple.com/HT207922	O-APP-MAC O--010817/263
Denial of	20-07-2017	6.8	An issue was discovered in certain Apple	https://sup	O-APP-

Service; Overflow; Memory Corruption Gain Information			products. macOS before 10.12.6 is affected. The issue involves the "Audio" component. It allows remote attackers to obtain sensitive information from process memory or cause a denial of service (memory corruption) via a crafted audio file. **CVE ID: CVE-2017-7015**	port.apple.com/HT207922	MAC O--010817/264
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	7.9	An issue was discovered in certain Apple products. macOS before 10.12.6 is affected. The issue involves the "Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7054**	https://support.apple.com/HT207922	O-APP-MAC O--010817/265
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	7.9	An issue was discovered in certain Apple products. macOS before 10.12.6 is affected. The issue involves the "Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7051**	https://support.apple.com/HT207922	O-APP-MAC O--010817/266
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	7.9	An issue was discovered in certain Apple products. macOS before 10.12.6 is affected. The issue involves the "Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7050**	https://support.apple.com/HT207922	O-APP-MAC O--010817/267
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.6 is affected. The issue involves the "Intel Graphics Driver" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7044**	https://support.apple.com/HT207922	O-APP-MAC O--010817/268
Denial of Service; Execute Code;	20-07-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.6 is affected. The issue involves the "Intel	https://support.apple.com/HT207	O-APP-MAC O--010817/

Overflow; Memory Corruption			Graphics Driver" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7035**	922	269
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.6 is affected. The issue involves the "kext tools" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7032**	https://support.apple.com/HT207922	O-APP-MAC O--010817/270
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.6 is affected. The issue involves the "AppleGraphicsPowerManagement" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7021**	https://support.apple.com/HT207922	O-APP-MAC O--010817/271
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.6 is affected. The issue involves the "Intel Graphics Driver" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7017**	https://support.apple.com/HT207922	O-APP-MAC O--010817/272
Denial of Service; Execute Code; Overflow; Memory Corruption	20-07-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.6 is affected. The issue involves the "Intel Graphics Driver" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-7014**	https://support.apple.com/HT207922	O-APP-MAC O--010817/273

Asuswrt-merlin Project

Rt Ac1200g Firmware;Rt Ac1200gu Firmware;Rt Ac1900p Firmware;Rt N12+ Pro Firmware;Rt-ac1200 Firmware;Rt-ac3100 Firmware;Rt-ac3200 Firmware;Rt-ac51u Firmware;Rt-ac52u Firmware;Rt-ac53 Firmware;Rt-ac5300 Firmware;Rt-ac55u Firmware;Rt-ac56u Firmware;Rt-ac58u Firmware;Rt-ac66u B1 Firmware;Rt-ac66u Firmware;Rt-ac68p Firmware;Rt-ac68u Firmware;Rt-ac88u Firmware;Rt-n12+ Firmware;Rt-n12d1 Firmware;Rt-n12hp B1 Firmware;Rt-

n12hp Firmware;Rt-n16 Firmware;Rt-n18u Firmware;Rt-n300 Firmware;Rt-n56u Firmware;Rt-n66u Firmware					
Execute Code; Overflow	17-07-2017	6.8	Stack buffer overflow in networkmap in Asuswrt-Merlin firmware for ASUS devices and ASUS firmware for ASUS RT-AC5300, RT_AC1900P, RT-AC68U, RT-AC68P, RT-AC88U, RT-AC66U, RT-AC66U_B1, RT-AC58U, RT-AC56U, RT-AC55U, RT-AC52U, RT-AC51U, RT-N18U, RT-N66U, RT-N56U, RT-AC3200, RT-AC3100, RT_AC1200GU, RT_AC1200G, RT-AC1200, RT-AC53, RT-N12HP, RT-N12HP_B1, RT-N12D1, RT-N12+, RT_N12+_PRO, RT-N16, and RT-N300 devices allows remote attackers to execute arbitrary code on the router by hosting a crafted device description XML document (that includes a serviceType element) at a URL specified within a Location header in an SSDP response. **CVE ID: CVE-2017-11345**	http://www.openwall.com/lists/oss-security/2017/07/14/3	O-ASU-RT AC--010817/274
Execute Code; Overflow	17-07-2017	9.3	Global buffer overflow in networkmap in Asuswrt-Merlin firmware for ASUS devices and ASUS firmware for ASUS RT-AC5300, RT_AC1900P, RT-AC68U, RT-AC68P, RT-AC88U, RT-AC66U, RT-AC66U_B1, RT-AC58U, RT-AC56U, RT-AC55U, RT-AC52U, RT-AC51U, RT-N18U, RT-N66U, RT-N56U, RT-AC3200, RT-AC3100, RT_AC1200GU, RT_AC1200G, RT-AC1200, RT-AC53, RT-N12HP, RT-N12HP_B1, RT-N12D1, RT-N12+, RT_N12+_PRO, RT-N16, and RT-N300 devices allows remote attackers to write shellcode at any address in the heap; this can be used to execute arbitrary code on the router by hosting a crafted device description XML document at a URL specified within a Location header in an SSDP response. **CVE ID: CVE-2017-11344**	http://www.openwall.com/lists/oss-security/2017/07/14/3	O-ASU-RT AC--010817/275
Execute Code; Overflow	18-07-2017	10	Stack-based buffer overflow in ASUS_Discovery.c in networkmap in Asuswrt-Merlin firmware for ASUS devices and ASUS firmware for ASUS RT-AC5300, RT_AC1900P, RT-AC68U, RT-AC68P, RT-AC88U, RT-AC66U, RT-	http://www.openwall.com/lists/oss-security/2017/07/13/	O-ASU-RT AC--010817/276

			AC66U_B1, RT-AC58U, RT-AC56U, RT-AC55U, RT-AC52U, RT-AC51U, RT-N18U, RT-N66U, RT-N56U, RT-AC3200, RT-AC3100, RT_AC1200GU, RT_AC1200G, RT-AC1200, RT-AC53, RT-N12HP, RT-N12HP_B1, RT-N12D1, RT-N12+, RT_N12+_PRO, RT-N16, and RT-N300 devices allows remote attackers to execute arbitrary code via long device information that is mishandled during a strcat to a device list. **CVE ID: CVE-2017-11420**	1	
Buffalo					
Wapm-1166d Firmware; Wapm-apg600h Firmware					
Bypass	21-07-2017	10	WAPM-1166D firmware Ver.1.2.7 and earlier, WAPM-APG600H firmware Ver.1.16.1 and earlier allows remote attackers to bypass authentication and access the configuration interface via unspecified vectors. **CVE ID: CVE-2017-2126**	http://buffalo.jp/support_s/s20170718.html	O-BUF-WAPM---010817/277
Cisco					
Dpc3928ad Docsis Wireless Router Firmware					
Gain Information	20-07-2017	5	Technicolor DPC3928AD DOCSIS devices allow remote attackers to read arbitrary files via a request starting with "GET /../" on TCP port 4321. **CVE ID: CVE-2017-11502**	https://blogs.securiteam.com/index.php/archives/2911#more-2911	O-CIS-DPC39--010817/278
IOS					
Execute Code; Overflow	17-07-2017	9	The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.2 through 3.17 contains multiple vulnerabilities that could allow an authenticated, remote attacker to remotely execute code on an affected system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities. The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp	O-CIS-IOS--010817/279

			software. The vulnerabilities affect all versions of SNMP: Versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP Version 2c or earlier, the attacker must know the SNMP read-only community string for the affected system. To exploit these vulnerabilities via SNMP Version 3, the attacker must have user credentials for the affected system. All devices that have enabled SNMP and have not explicitly excluded the affected MIBs or OIDs should be considered vulnerable. Cisco Bug IDs: CSCve78027, CSCve60276. **CVE ID: CVE-2017-6744**		
Execute Code; Overflow	17-07-2017	9	The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.2 through 3.17 contains multiple vulnerabilities that could allow an authenticated, remote attacker to remotely execute code on an affected system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities. The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected software. The vulnerabilities affect all versions of SNMP: Versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP Version 2c or earlier, the attacker must know the SNMP read-only community string for the affected system. To exploit these vulnerabilities via SNMP Version 3, the attacker must have user credentials for the affected system. All devices that have enabled SNMP and have not explicitly excluded the affected MIBs or OIDs should be considered vulnerable. Cisco Bug IDs: CSCve60376, CSCve78027. **CVE ID: CVE-2017-6743**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp	O-CIS-IOS--010817/280
Execute Code; Overflow	17-07-2017	9	The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS 12.0 through 12.4 and 15.0 through 15.6	https://tools.cisco.com/security/ce	O-CIS-IOS--010817/

			and IOS XE 2.2 through 3.17 contains multiple vulnerabilities that could allow an authenticated, remote attacker to remotely execute code on an affected system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities. The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected software. The vulnerabilities affect all versions of SNMP: Versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP Version 2c or earlier, the attacker must know the SNMP read-only community string for the affected system. To exploit these vulnerabilities via SNMP Version 3, the attacker must have user credentials for the affected system. All devices that have enabled SNMP and have not explicitly excluded the affected MIBs or OIDs should be considered vulnerable. Cisco Bug IDs: CSCve66601. **CVE ID: CVE-2017-6740**	nter/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp	281
Execute Code; Overflow	17-07-2017	9	The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.2 through 3.17 contains multiple vulnerabilities that could allow an authenticated, remote attacker to remotely execute code on an affected system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities. The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected software. The vulnerabilities affect all versions of SNMP: Versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP Version 2c or earlier, the attacker must	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp	O-CIS-IOS--010817/282

			know the SNMP read-only community string for the affected system. To exploit these vulnerabilities via SNMP Version 3, the attacker must have user credentials for the affected system. All devices that have enabled SNMP and have not explicitly excluded the affected MIBs or OIDs should be considered vulnerable. Cisco Bug IDs: CSCve66540. **CVE ID: CVE-2017-6739**		
Execute Code; Overflow	17-07-2017	9	The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.2 through 3.17 contains multiple vulnerabilities that could allow an authenticated, remote attacker to remotely execute code on an affected system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities. The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected software. The vulnerabilities affect all versions of SNMP: Versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP Version 2c or earlier, the attacker must know the SNMP read-only community string for the affected system. To exploit these vulnerabilities via SNMP Version 3, the attacker must have user credentials for the affected system. All devices that have enabled SNMP and have not explicitly excluded the affected MIBs or OIDs should be considered vulnerable. Cisco Bug IDs: CSCve89865, CSCsy56638. **CVE ID: CVE-2017-6738**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp	O-CIS-IOS--010817/283
Execute Code; Overflow	17-07-2017	9	The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.2 through 3.17 contains multiple vulnerabilities that could allow an authenticated, remote attacker to remotely execute code on an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IOS--010817/284

			system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities. The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected software. The vulnerabilities affect all versions of SNMP: Versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP Version 2c or earlier, the attacker must know the SNMP read-only community string for the affected system. To exploit these vulnerabilities via SNMP Version 3, the attacker must have user credentials for the affected system. All devices that have enabled SNMP and have not explicitly excluded the affected MIBs or OIDs should be considered vulnerable. Cisco Bug IDs: CSCve60402. **CVE ID: CVE-2017-6737**	20170629-snmp	
Execute Code; Overflow	17-07-2017	9	The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.2 through 3.17 contains multiple vulnerabilities that could allow an authenticated, remote attacker to remotely execute code on an affected system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities. The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected software. The vulnerabilities affect all versions of SNMP: Versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP Version 2c or earlier, the attacker must know the SNMP read-only community string for the affected system. To exploit these vulnerabilities via SNMP Version 3, the attacker must have user credentials	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp	O-CIS-IOS--010817/285

			for the affected system. All devices that have enabled SNMP and have not explicitly excluded the affected MIBs or OIDs should be considered vulnerable. Cisco Bug IDs: CSCve57697. **CVE ID: CVE-2017-6736**		
Ios Xe					
Execute Code; Overflow	17-07-2017	9	The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.2 through 3.17 contains multiple vulnerabilities that could allow an authenticated, remote attacker to remotely execute code on an affected system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities. The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected software. The vulnerabilities affect all versions of SNMP: Versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP Version 2c or earlier, the attacker must know the SNMP read-only community string for the affected system. To exploit these vulnerabilities via SNMP Version 3, the attacker must have user credentials for the affected system. All devices that have enabled SNMP and have not explicitly excluded the affected MIBs or OIDs should be considered vulnerable. Cisco Bug IDs: CSCve54313. **CVE ID: CVE-2017-6742**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp	O-CIS-IOS X--010817/286
Execute Code; Overflow	17-07-2017	9	The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.2 through 3.17 contains multiple vulnerabilities that could allow an authenticated, remote attacker to remotely execute code on an affected system or cause an affected system to reload. An attacker could exploit these vulnerabilities by sending a crafted	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp	O-CIS-IOS X--010817/287

			SNMP packet to an affected system via IPv4 or IPv6. Only traffic directed to an affected system can be used to exploit these vulnerabilities. The vulnerabilities are due to a buffer overflow condition in the SNMP subsystem of the affected software. The vulnerabilities affect all versions of SNMP: Versions 1, 2c, and 3. To exploit these vulnerabilities via SNMP Version 2c or earlier, the attacker must know the SNMP read-only community string for the affected system. To exploit these vulnerabilities via SNMP Version 3, the attacker must have user credentials for the affected system. All devices that have enabled SNMP and have not explicitly excluded the affected MIBs or OIDs should be considered vulnerable. Cisco Bug IDs: CSCve66658. **CVE ID: CVE-2017-6741**		
Datataker					
Dt8x Firmware					
NA	17-07-2017	5	dataTaker DT8x dEX 1.72.007 allows remote attackers to compose programs or schedules, for purposes such as sending e-mail messages or making outbound connections to FTP servers for uploading data. **CVE ID: CVE-2017-11349**	NA	O-DAT-DT8X --010817/288
Freebsd					
Freebsd					
DoS	25-07-2017	5	The inet module in FreeBSD 10.2x before 10.2-PRERELEASE, 10.2-BETA2-p2, 10.2-RC1-p1, 10.1x before 10.1-RELEASE-p16, 9.x before 9.3-STABLE, 9.3-RELEASE-p21, and 8.x before 8.4-STABLE, 8.4-RELEASE-p35 on systems with VNET enabled and at least 16 VNET instances allows remote attackers to cause a denial of service (mbuf consumption) via multiple concurrent TCP connections. **CVE ID: CVE-2015-1417**	NA	O-FRE-FREEB--010817/289
Geneko					
Gwr202 Gprs Router Firmware; Gwr252 Edge Router Firmware; Gwr352 3g Router Firmware; Gwr352wv Wide Voltage 3g Router Firmware					
Directory	19-07-2017	5	Geneko GWR routers allow directory	https://blog	O-GEN-

Traversal			traversal sequences starting with a /../ substring, as demonstrated by unauthenticated read access to the configuration file. **CVE ID: CVE-2017-11456**	s.securitea m.com/inde x.php/archi ves/3317# more-3317	GWR20--010817/290
Google					
Android					
Bypass	17-07-2017	7.2	Android 6.0 has an authentication bypass for attackers with root and physical access. Cryptographic authentication tokens (AuthTokens) used by the Trusted Execution Environment (TEE) are protected by a weak challenge. This allows adversaries to replay previously captured responses and use the TEE without authenticating. All apps using authentication-gated cryptography are vulnerable to this attack, which was confirmed on the LG Nexus 5X. **CVE ID: CVE-2016-10398**	https://ho mepages.sta ff.os3.nl/~d elaat/rp/20 15-2016/p30/r eport.pdf	O-GOO-ANDRO--010817/291
Greenpacket					
Dx-350 Firmware					
CSRF	21-07-2017	6.8	Cross-Site Request Forgery (CSRF) exists in Green Packet DX-350 Firmware version v2.8.9.5-g1.4.8-atheeb, as demonstrated by a request to ajax.cgi that enables UPnP. **CVE ID: CVE-2017-9930**	https://isco uncil.blogsp ot.com/201 7/07/green -packet-dx-350-vulnerable-to-csrf.html	O-GRE-DX-35--010817/292
NA	21-07-2017	7.5	In Green Packet DX-350 Firmware version v2.8.9.5-g1.4.8-atheeb, the "PING" (aka tag_ipPing) feature within the web interface allows performing command injection, via the "pip" parameter. **CVE ID: CVE-2017-9980**	https://isco uncil.blogsp ot.com/201 7/07/comm and-injection-in-green-packet-dx.html	O-GRE-DX-35--010817/293
NA	21-07-2017	7.5	Green Packet DX-350 Firmware version v2.8.9.5-g1.4.8-atheeb has a default password of admin for the admin account. **CVE ID: CVE-2017-9932**	https://isco uncil.blogsp ot.com/201 7/07/authe ntication-bypass-in-green-	O-GRE-DX-35--010817/294

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

				packet.html	
Humax					
Hg100r Firmware					
Bypass; Gain Information	19-07-2017	7.5	The Humax Wi-Fi Router model HG100R-* 2.0.6 is prone to an authentication bypass vulnerability via specially crafted requests to the management console. The bug is exploitable remotely when the router is configured to expose the management console. The router is not validating the session token while returning answers for some methods in url '/api'. An attacker can use this vulnerability to retrieve sensitive information such as private/public IP addresses, SSID names, and passwords. **CVE ID: CVE-2017-11435**	https://hackertor.com/2017/07/19/na-CVE-2017-11435-the-humax-wi-fi-router-model-hg100r-2-0-6-is/	O-HUM-HG100--010817/295
Intenogroup					
Inteno Router Firmware					
NA	17-07-2017	9	Inteno routers have a JUCI ACL misconfiguration that allows the "user" account to read files, write to files, and add root SSH keys via JSON commands to ubus. (Exploitation is sometimes easy because the "user" password might be "user" or might match the Wi-Fi key.) **CVE ID: CVE-2017-11361**	https://neonsea.uk/blog/2017/07/17/CVE-2017-11361.html	O-INT-INTEN--010817/296
Juniper					
Junos					
DoS	17-07-2017	5	On all vSRX and SRX Series devices, when the DHCP or DHCP relay is configured, specially crafted packet might cause the flowd process to crash, halting or interrupting traffic from flowing through the device(s). Repeated crashes of the flowd process may constitute an extended denial of service condition for the device(s). If the device is configured in high-availability, the RG1+ (data-plane) will fail-over to the secondary node. If the device is configured in stand-alone, there will be temporary traffic interruption until the flowd process is restored automatically. Sustained crafted packets may cause the secondary	https://kb.juniper.net/JSA10789	O-JUN-JUNOS--010817/297

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

			failover node to fail back, or fail completely, potentially halting flowd on both nodes of the cluster or causing flip-flop failovers to occur. No other Juniper Networks products or platforms are affected by this issue. Affected releases are Juniper Networks Junos OS 12.1X46 prior to 12.1X46-D67 on vSRX or SRX Series; 12.3X48 prior to 12.3X48-D50 on vSRX or SRX Series; 15.1X49 prior to 15.1X49-D91, 15.1X49-D100 on vSRX or SRX Series. **CVE ID: CVE-2017-10605**		
NA	17-07-2017	7.2	An XML injection vulnerability in Junos OS CLI can allow a locally authenticated user to elevate privileges and run arbitrary commands as the root user. This issue was found during internal product security testing. Affected releases are Juniper Networks Junos OS 15.1X53 prior to 15.1X53-D47, 15.1 prior to 15.1R3. Junos versions prior to 15.1 are not affected. No other Juniper Networks products or platforms are affected by this issue. **CVE ID: CVE-2017-10603**	https://kb.juniper.net/JSA10805	O-JUN-JUNOS--010817/298
Execute Code; Overflow	17-07-2017	7.2	A buffer overflow vulnerability in Junos OS CLI may allow a local authenticated user with read only privileges and access to Junos CLI, to execute code with root privileges. Affected releases are Juniper Networks Junos OS 14.1X53; 14.2 prior to 14.2R6; 15.1 prior to 15.1F5, 15.1F6, 15.1R3; 15.1X49 prior to 15.1X49-D40; 15.1X53 prior to 15.1X53-D47, 15.1X53-D70. This issue does not affect Junos 14.1 or prior releases. No other Juniper Networks products or platforms are affected by this issue. **CVE ID: CVE-2017-10602**	https://kb.juniper.net/JSA10803	O-JUN-JUNOS--010817/299
Gain Privileges	17-07-2017	7.2	An insufficient authentication vulnerability on platforms where Junos OS instances are run in a virtualized environment, may allow unprivileged users on the Junos OS instance to gain access to the host operating environment, and thus escalate	https://kb.juniper.net/JSA10787	O-JUN-JUNOS--010817/300

			privileges. Affected releases are Juniper Networks Junos OS 14.1X53 prior to 14.1X53-D40 on QFX5110, QFX5200, QFX10002, QFX10008, QFX10016, EX4600 and NFX250; 15.1 prior to 15.1R5 on EX4600; 15.1X49 prior to 15.1X49-D70 on vSRX, SRX1500, SRX4100, SRX4200; 16.1 prior to 16.1R2 on EX4600, ACX5000 series. This issue does not affect vMX. No other Juniper Networks products or platforms are affected by this issue. **CVE ID: CVE-2017-2341**		
Execute Code	17-07-2017	9	A command injection vulnerability in the IDP feature of Juniper Networks Junos OS on SRX series devices potentially allows a user with login access to the device to execute shell commands and elevate privileges. Affected releases are Juniper Networks Junos OS 12.1X44 prior to 12.1X44-D60; 12.1X46 prior to 12.1X46-D50; 12.1X47 prior to 12.1X47-D30, 12.1X47-D35; 12.3X48 prior to 12.3X48-D20, 12.3X48-D30; 15.1X49 prior to 15.1X49-D20, 15.1X49-D30. **CVE ID: CVE-2017-2349**	https://kb.juniper.net/JSA10801	O-JUN-JUNOS--010817/301
NA	17-07-2017	10	A specific device configuration can result in a commit failure condition. When this occurs, a user is logged in without being prompted for a password while trying to login through console, ssh, ftp, telnet or su, etc., This issue relies upon a device configuration precondition to occur. Typically, device configurations are the result of a trusted administrative change to the system's running configuration. The following error messages may be seen when this failure occurs: mgd: error: commit failed: (statements constraint check failed) Warning: Commit failed, activating partial configuration. Warning: Edit the router configuration to fix these errors. If the administrative changes are not made that result in such a failure, then this issue is not seen. No other Juniper Networks products or platforms are	https://kb.juniper.net/JSA10802	O-JUN-JUNOS--010817/302

			affected by this issue. Affected releases are Juniper Networks Junos OS 12.3 prior to 12.3R10, 12.3R11; 12.3X48 prior to 12.3X48-D20; 13.2 prior to 13.2R8; 13.3 prior to 13.3R7; 14.1 prior to 14.1R4-S12, 14.1R5, 14.1R6; 14.1X53 prior to 14.1X53-D30; 14.2 prior to 14.2R4; 15.1 prior to 15.1F2, 15.1F3, 15.1R2. **CVE ID: CVE-2017-10601**		
NA	17-07-2017	10	The Integrated User Firewall (UserFW) feature was introduced in Junos OS version 12.1X47-D10 on the Juniper SRX Series devices to provide simple integration of user profiles on top of the existing firewall polices. As part of an internal security review of the UserFW services authentication API, hardcoded credentials were identified and removed which can impact both the SRX Series device, and potentially LDAP and Active Directory integrated points. An attacker may be able to completely compromise SRX Series devices, as well as Active Directory servers and services. When Active Directory is compromised, it may allow access to user credentials, workstations, servers performing other functions such as email, database, etc. Inter-Forest Active Directory deployments may also be at risk as the attacker may gain full administrative control over one or more Active Directories depending on the credentials supplied by the administrator of the AD domains and SRX devices performing integrated authentication of users, groups and devices. To identify if your device is potentially vulnerable to exploitation, check to see if the service is operating; from CLI review the following output: root@SRX-Firewall# run show services user-identification active-directory-access domain-controller status extensive A result of "Status: Connected" will indicate that the service is active on the device. To evaluate if user authentication is occurring through the	https://kb.juniper.net/JSA10791	O-JUN-JUNOS--010817/303

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

			device: root@SRX-Firewall# run show services user-identification active-directory-access active-directory-authentication-table all Next review the results to see if valid users and groups are returned. e.g. Domain: juniperlab.com Total entries: 3 Source IP Username groups state 172.16.26.1 administrator Valid 192.168.26.2 engg01 engineers Valid 192.168.26.3 guest01 guests Valid Domain: NULL Total entries: 8 Source IP Username groups state 192.168.26.4 Invalid 192.168.26.5 Invalid This will also indicate that Valid users and groups are authenticating through the device. Affected releases are Juniper Networks Junos OS 12.3X48 from 12.3X48-D30 and prior to 12.3X48-D35 on SRX series; 15.1X49 from 15.1X49-D40 and prior to 15.1X49-D50 on SRX series. Devices on any version of Junos OS 12.1X46, or 12.1X47 are unaffected by this issue. **CVE ID: CVE-2017-2343**		
Linux					
Kernel					
Overflow	17-07-2017	7.2	Linux drivers/char/lp.c Out-of-Bounds Write. Due to a missing bounds check, and the fact that parport_ptr integer is static, a 'secure boot' kernel command line adversary (can happen due to bootloader vulns, e.g. Google Nexus 6's CVE-2016-10277, where due to a vulnerability the adversary has partial control over the command line) can overflow the parport_nr array in the following code, by appending many (>LP_NO) 'lp=none' arguments to the command line. **CVE ID: CVE-2017-1000363**	NA	O-LIN-KERNE--010817/304
DoS	24-07-2017	6.9	net/xfrm/xfrm_policy.c in the Linux kernel through 4.12.3, when CONFIG_XFRM_MIGRATE is enabled, does not ensure that the dir value of xfrm_userpolicy_id is XFRM_POLICY_MAX or less, which allows local users to cause a denial of service	http://seclists.org/bugtraq/2017/Jul/30	O-LIN-LINUX--010817/305

			(out-of-bounds access) or possibly have unspecified other impact via an XFRM_MSG_MIGRATE xfrm Netlink message. **CVE ID: CVE-2017-11600**		
Overflow Gain Privileges	20-07-2017	7.2	Buffer overflow in the mp_override_legacy_irq() function in arch/x86/kernel/acpi/boot.c in the Linux kernel through 4.12.2 allows local users to gain privileges via a crafted ACPI table. **CVE ID: CVE-2017-11473**	https://git.kernel.org/pub/scm/linux/kernel/git/tip/tip.git/commit/?id=70ac67826602edf8c0ccb413e5ba7eacf597a60c	O-LIN-LINUX--010817/306
Denial of Service; Overflow Gain Privileges	25-07-2017	7.2	The brcmf_cfg80211_mgmt_tx function in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux kernel before 4.12.3 allows local users to cause a denial of service (buffer overflow and system crash) or possibly gain privileges via a crafted NL80211_CMD_FRAME Netlink packet. **CVE ID: CVE-2017-7541**	https://www.spinics.net/lists/stable/msg180994.html	O-LIN-LINUX--010817/307
Onosproject					
Onos					
Execute Code	17-07-2017	7.5	Linux foundation ONOS 1.9.0 is vulnerable to unauthenticated upload of applications (.oar) resulting in remote code execution **CVE ID: CVE-2017-1000081**	https://jira.onosproject.org/secure/Dashboard.jspa	O-ONO-ONOS--010817/308
NA	17-07-2017	7.5	Linux foundation ONOS 1.9.0 allows unauthenticated use of websockets **CVE ID: CVE-2017-1000080**	https://jira.onosproject.org/secure/Dashboard.jspa	O-ONO-ONOS--010817/309
NA	17-07-2017	7.8	Linux foundation ONOS 1.9.0 is vulnerable to a DoS **CVE ID: CVE-2017-1000079**	https://jira.onosproject.org/secure/Dashboard.jspa	O-ONO-ONOS--010817/310
Sony					
Wg-c10 Firmware					
Execute Code;	21-07-2017	9	Buffer overflow in WG-C10 v3.0.79 and	NA	O-SON-

Overflow			earlier allows an attacker to execute arbitrary commands via unspecified vectors. **CVE ID: CVE-2017-2276**		WG-C1--010817/311
Execute Code	21-07-2017	9	WG-C10 v3.0.79 and earlier allows an attacker to execute arbitrary OS commands via unspecified vectors. **CVE ID: CVE-2017-2275**	NA	O-SON-WG-C1--010817/312
Televes					
Coaxdata Gateway 1gbps Firmware					
NA	20-07-2017	5	Televes COAXDATA GATEWAY 1Gbps devices doc-wifi-hgw_v1.02.0014 4.20 have cleartext credentials in /mib.db. **CVE ID: CVE-2017-6532**	NA	O-TEL-COAXD--010817/313
NA	20-07-2017	5	On Televes COAXDATA GATEWAY 1Gbps devices doc-wifi-hgw_v1.02.0014 4.20, the backup/restore feature lacks access control, related to ReadFile.cgi and LoadCfgFile. **CVE ID: CVE-2017-6531**	NA	O-TEL-COAXD--010817/314
NA	20-07-2017	5	Televes COAXDATA GATEWAY 1Gbps devices doc-wifi-hgw_v1.02.0014 4.20 do not check password.shtml authorization, leading to Arbitrary password change. **CVE ID: CVE-2017-6530**	NA	O-TEL-COAXD--010817/315
Tp-link					
Archer C9 (2.0) Firmware					
NA	21-07-2017	5	passwd_recovery.lua on the TP-Link Archer C9(UN)_V2_160517 allows an attacker to reset the admin password by leveraging a predictable random number generator seed. This is fixed in C9(UN)_V2_170511. **CVE ID: CVE-2017-11519**	NA	O-TP--ARCHE--010817/316
Operating System; Application (OS / A)					
Canonical; Debian; Fedoraproject; Novell; Opensuse Project; Redhat; Suse / NTP ; Suse					
Ubuntu Linux/Debian Linux/Fedora/Leap/Opensuse/Enterprise Linux Desktop;Enterprise Linux Hpc Node;Enterprise Linux Hpc Node Eus;Enterprise Linux Server;Enterprise Linux Server Eus;Enterprise Linux Workstation/Linux Enterprise Desktop;Linux Enterprise Server;Linux Enterprise Software Development Kit;Manager;Manager Proxy;Openstack Cloud/NTP/Linux Enterprise Debuginfo					
DoS	21-07-2017	5	The panic_gate check in NTP before 4.2.8p5 is only re-enabled after the first change to the system clock that was greater than 128 milliseconds by default, which allows remote attackers to set	https://www.oracle.com/technetwork/topics/security/lin	O-A-CAN-UBUNT--010817/317

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): DoS - Denial of Service; CSRF - Cross Site Request Forgery; XSS - Cross Site Scripting; Sql - SQL Injection; NA: Not Applicable

			NTP to an arbitrary time when started with the -g option, or to alter the time by up to 900 seconds otherwise by responding to an unspecified number of requests from trusted sources, and leveraging a resulting denial of service (abort and restart). **CVE ID: CVE-2015-5300**	uxbulletinoct2015-2719645.html	
Canonical;Debian;Fedoraproject;Novell;Redhat;Suse/NTP;Suse					
Ubuntu Linux/Debian Linux/Fedora/Leap/Enterprise Linux Desktop;Enterprise Linux Hpc Node;Enterprise Linux Server;Enterprise Linux Workstation/Linux Enterprise Server;Manager;Manager Proxy;Openstack Cloud/NTP/Linux Enterprise Debuginfo					
DoS	21-07-2017	5	The ULOGTOD function in ntp.d in SNTP before 4.2.7p366 does not properly perform type conversions from a precision value to a double, which allows remote attackers to cause a denial of service (infinite loop) via a crafted NTP packet. **CVE ID: CVE-2015-5219**	https://www.ibm.com/support/home/docdisplay?lndocid=migr-5099409	O-A-CAN-UBUNT--010817/318
Canonical; Debian; Fedoraproject; Redhat / NTP					
Ubuntu Linux/Debian Linux/Fedora/Enterprise Linux Desktop;Enterprise Linux Hpc Node;Enterprise Linux Server;Enterprise Linux Workstation/NTP					
DoS	21-07-2017	5	ntp_openssl.m4 in ntpd in NTP before 4.2.7p112 allows remote attackers to cause a denial of service (segmentation fault) via a crafted statistics or filegen configuration command that is not enabled during compilation. **CVE ID: CVE-2015-5195**	https://github.com/ntp-project/ntp/commit/52e977d79a0c4ace997e5c74af429844da2f27be	O-A-CAN-UBUNT--010817/319
Canonical; Debian; Fedoraproject; Redhat; Suse/ NTP; Suse					
Ubuntu Linux / Debian Linux / Fedora / Enterprise Linux Desktop; Enterprise Linux Hpc Node; Enterprise Linux Server; Enterprise Linux Workstation/ Linux Enterprise Server; Manager; Manager Proxy; Openstack Cloud/ NTP/ Linux Enterprise Debuginfo					
DoS	21-07-2017	5	The log_config_command function in ntp_parser.y in ntpd in NTP before 4.2.7p42 allows remote attackers to cause a denial of service (ntpd crash) via crafted logconfig commands. **CVE ID: CVE-2015-5194**	http://bk1.ntp.org/ntp-dev/?PAGE=patch&REV=4c4fc141LwvcoGp-lLGhkAFp3ZvtrA	O-A-CAN-UBUNT--010817/320