Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Acer					
Acer Portal					
NA	08-06-2017	4.3	Acer Portal app before 3.9.4.2000 for Android does not properly validate SSL certificates, which allows remote attackers to perform a Man-in-the-middle attack via a crafted SSL certificate. **CVE ID: CVE-2016-5648**	NA	A-ACE-ACER - 210617/01
Adblock					
Adblock					
NA	08-06-2017	6.4	AdBlock before 2.21 allows remote attackers to block arbitrary resources on arbitrary websites and to disable arbitrary blocking filters. **CVE ID: CVE-2015-2692**	https://github.com/kzar/watchadblock/commit/5b77de6ea77e0eff2aa726d9722d64fb4964b985	A-ADB-ADBLO-210617/02
AMD					
Fglrx-driver					
Gain Privileges	07-06-2017	7.2	AMD fglrx-driver before 15.9 allows local users to gain Gain Privilegesileges via a symlink attack. NOTE: This vulnerability exists due to an incomplete fix for CVE-2015-7723. **CVE ID: CVE-2015-7724**	NA	A-AMD-FGLRX-210617/03
Gain Privileges	07-06-2017	7.2	AMD fglrx-driver before 15.7 allows local users to gain Gain Privilegesileges via a symlink attack. **CVE ID: CVE-2015-7723**	NA	A-AMD-FGLRX-210617/04
Ansibleworks					
Ansible					
Execute Code	08-06-2017	6.5	The user module in ansible	https://github.	A-ANS-

			before 1.6.6 allows remote authenticated users to execute arbitrary commands. **CVE ID: CVE-2014-3498**	com/ansible/ansible/commit/8ed6350e65c82292a631f08845dfaacffe7f07f5	ANSIB-210617/05
NA	07-06-2017	7.2	The chroot, jail, and zone connection plugins in ansible before 1.9.2 allow local users to escape a restricted environment via a symlink attack. **CVE ID: CVE-2015-6240**	https://bugzilla.redhat.com/show_bug.cgi?id=1243468	A-ANS-ANSIB-210617/06
Apache					
Cxf Fediz					
DoS	07-06-2017	5	Application plugins in Apache CXF Fediz before 1.1.3 and 1.2.x before 1.2.1 allow remote attackers to cause a denial of service. **CVE ID: CVE-2015-5175**	https://git-wip-us.apache.org/repos/asf?p=cxf-fediz.git;a=commit;h=f65c961ea31e3c1851daba8e7e49fc37bbf77b19	A-APA-CXF F-210617/07
Hadoop					
NA	04-06-2017	8.5	In Apache Hadoop 2.8.0, 3.0.0-alpha1, and 3.0.0-alpha2, the LinuxContainerExecutor runs docker commands as root with insufficient input validation. When the docker feature is enabled, authenticated users can run commands as root. **CVE ID: CVE-2017-7669**	NA	A-APA-HADOO-210617/08
Nifi					
XSS	12-06-2017	4.3	In Apache NiFi before 0.7.4 and 1.x before 1.3.0, there are certain user input components in the UI which had been guarding for some forms of XSS issues but were insufficient. **CVE ID: CVE-2017-7665**	NA	A-APA-NIFI-210617/09
NA	12-06-2017	5	Apache NiFi before 0.7.4 and 1.x	NA	A-APA-

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

			before 1.3.0 need to establish the response header telling browsers to only allow framing with the same origin. **CVE ID: CVE-2017-7667**		NIFI-210617/10
Ranger					
NA	14-06-2017	4.3	In environments that use external location for hive tables, Hive Authorizer in Apache Ranger before 0.7.1 should be checking RWX permission for create table. **CVE ID: CVE-2017-7677**	https://cwiki.apache.org/confluence/display/RANGER/Vulnerabilities+found+in+Ranger	A-APA-RANGE-210617/11
NA	14-06-2017	4.3	Apache Ranger before 0.6.3 policy engine incorrectly matches paths in certain conditions when policy does not contain wildcards and has recursion flag set to true. **CVE ID: CVE-2016-8746**	https://cwiki.apache.org/confluence/display/RANGER/Vulnerabilities+found+in+Ranger	A-APA-RANGE-210617/12
NA	14-06-2017	7.5	Policy resource matcher in Apache Ranger before 0.7.1 ignores characters after '*' wildcard character - like my*test, test*.txt. This can result in unintended behavior. **CVE ID: CVE-2017-7676**	https://cwiki.apache.org/confluence/display/RANGER/Vulnerabilities+found+in+Ranger	A-APA-RANGE-210617/13
Tomcat					
NA	06-06-2017	5	The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the error page. This means that the request is presented to the error page with the original HTTP method. If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. The Default	NA	A-APA-TOMCA-210617/14

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

			Servlet in Apache Tomcat 9.0.0.M1 to 9.0.0.M20, 8.5.0 to 8.5.14, 8.0.0.RC1 to 8.0.43 and 7.0.0 to 7.0.77 did not do this. Depending on the original request this could lead to unexpected and undesirable results for static error pages including, if the DefaultServlet is configured to permit writes, the replacement or removal of the custom error page. Notes for other user provided error pages: (1) Unless explicitly coded otherwise, JSPs ignore the the HTTP method. JSPs used as error pages must must ensure that they handle any error dispatch as a GET request, regardless of the actual method. (2) By default, the response generated by a Servlet does depend on the HTTP method. Custom Servlets used as error pages must ensure that they handle any error dispatch as a GET request, regardless of the actual method. **CVE ID: CVE-2017-5664**		
Ws-xmlrpc					
DoS	06-06-2017	4.3	The Content-Encoding HTTP header feature in ws-xmlrpc 3.1.3 as used in Apache Archiva allows remote attackers to cause a denial of service (resource consumption) by decompressing a large file containing zeroes. **CVE ID: CVE-2016-5004**	NA	A-APA-WS-XM-210617/15
ARM					
Arm Trusted Firmware					
DoS	07-06-2017	5	In ARM Trusted Firmware through 1.3, the secure self-hosted invasive debug interface allows normal world attackers to cause a denial of service	https://github.com/ARM-software/arm-trusted-firmware/wiki	A-ARM-ARM T-210617/16

			(secure world panic) via vectors involving debug exceptions and debug registers. **CVE ID: CVE-2017-7564**	/ARM-Trusted-Firmware-Security-Advisory-TFV-2	
Bypass	07-06-2017	6.8	In ARM Trusted Firmware 1.3, RO memory is always executable at AArch64 Secure EL1, allowing attackers to bypass the MT_EXECUTE_NEVER protection mechanism. This issue occurs because of inconsistency in the number of execute-never bits (one bit versus two bits). **CVE ID: CVE-2017-7563**	https://github.com/ARM-software/arm-trusted-firmware/wiki/ARM-Trusted-Firmware-Security-Advisory-TFV-3	A-ARM-ARM T-210617/17
Arubanetworks					
Clearpass					
Sql	08-06-2017	7.5	SQL injection vulnerability in ClearPass Policy Manager 6.5.x through 6.5.6 and 6.6.0. **CVE ID: CVE-2016-2034**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2016-009.txt	A-ARU-CLEAR-210617/18
Asterisk					
Certified Asterisk;Open Source					
NA	02-06-2017	5	A memory exhaustion vulnerability exists in Asterisk Open Source 13.x before 13.15.1 and 14.x before 14.4.1 and Certified Asterisk 13.13 before 13.13-cert4, which can be triggered by sending specially crafted SCCP packets causing a infinite loop and leading to memory exhaustion (by message logging in that loop). **CVE ID: CVE-2017-9358**	https://bugs.debian.org/863906	A-AST-CERTI-210617/19
Atmail					
Atmail					
CSRF	08-06-2017	6.8	atmail before 7.8.0.2 has CSRF, allowing an attacker to create a user account. **CVE ID: CVE-2017-9519**	https://help.atmail.com/hc/en-us/articles/11	A-ATM-ATMAI-210617/20

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

				5007169147-Minor-Update-7-8-0-2-ActiveSync-2-3-6	
CSRF	08-06-2017	6.8	atmail before 7.8.0.2 has CSRF, allowing an attacker to change the SMTP hostname and hijack all emails. **CVE ID: CVE-2017-9518**	https://help.atmail.com/hc/en-us/articles/115007169147-Minor-Update-7-8-0-2-ActiveSync-2-3-6	A-ATM-ATMAI-210617/21
CSRF	08-06-2017	6.8	atmail before 7.8.0.2 has CSRF, allowing an attacker to upload and import users via CSV. **CVE ID: CVE-2017-9517**	https://help.atmail.com/hc/en-us/articles/115007169147-Minor-Update-7-8-0-2-ActiveSync-2-3-6	A-ATM-ATMAI-210617/22
Bigtreecms					
Bigtree Cms					
Directory Traversal	04-06-2017	5	A directory traversal vulnerability exists in core\admin\ajax\developer\extensions\file-browser.php in BigTree CMS through 4.2.18 on Windows, allowing attackers to read arbitrary files via ..\ sequences in the directory parameter. **CVE ID: CVE-2017-9428**	https://github.com/bigtreecms/BigTree-CMS/issues/289	A-BIG-BIGTR-210617/23
Execute Code; Sql	04-06-2017	6.5	SQL injection vulnerability in BigTree CMS through 4.2.18 allows remote authenticated users to execute arbitrary SQL commands via core\admin\modules\developer\modules\designer\form-create.php. The attacker creates a crafted table name at	https://github.com/bigtreecms/BigTree-CMS/issues/288	A-BIG-BIGTR-210617/24

			admin/developer/modules/designer/ and the injection is visible at admin/dashboard/vitals-statistics/integrity/check/?external=true. **CVE ID: CVE-2017-9427**		
Sql	05-06-2017	6.5	** DISPUTED ** BigTree CMS through 4.2.18 allows remote authenticated users to conduct SQL injection attacks via a crafted tables object in manifest.json in an uploaded package. This issue exists in core\admin\modules\developer\extensions\install\process.php and core\admin\modules\developer\packages\install\process.php. NOTE: the vendor states "You must implicitly trust any package or extension you install as they all have the ability to write PHP files." **CVE ID: CVE-2017-9443**	https://github.com/bigtreecms/BigTree-CMS/issues/292	A-BIG-BIGTR-210617/25
Execute Code	05-06-2017	6.5	** DISPUTED ** BigTree CMS through 4.2.18 allows remote authenticated users to execute arbitrary code by uploading a crafted package containing a PHP web shell, related to extraction of a ZIP archive to filename patterns such as cache/package/xxx/yyy.php. This issue exists in core\admin\modules\developer\extensions\install\unpack.php and core\admin\modules\developer\packages\install\unpack.php. NOTE: the vendor states "You must implicitly trust any package or extension you install as they all have the ability to write PHP files."	https://github.com/bigtreecms/BigTree-CMS/issues/291	A-BIG-BIGTR-210617/26

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

			CVE ID: CVE-2017-9442		
Execute Code Sql	06-06-2017	6.5	SQL injection vulnerability in BigTree CMS through 4.2.18 allows remote authenticated users to execute arbitrary SQL commands via core/admin/modules/developer/modules/views/create.php. The attacker creates a crafted table name at admin/developer/modules/views/create/ and the injection is visible at admin/ajax/auto-modules/views/searchable-page/ or admin/modules_name. **CVE ID: CVE-2017-9449**	https://github.com/bigtreecms/BigTree-CMS/issues/295	A-BIG-BIGTR-210617/27
CSRF	02-06-2017	6.8	Multiple CSRF issues exist in BigTree CMS through 4.2.18 - the clear parameter to core\admin\modules\dashboard\vitals-statistics\404\clear.php and the from or to parameter to core\admin\modules\dashboard\vitals-statistics\404\create-301.php. **CVE ID: CVE-2017-9379**	https://github.com/bigtreecms/BigTree-CMS/issues/287	A-BIG-BIGTR-210617/28
CSRF	02-06-2017	6.8	CSRF exists in BigTree CMS through 4.2.18 with the force parameter to /admin/pages/revisions.php - for example: /admin/pages/revisions/1/?force=false. A page with id=1 can be unlocked. **CVE ID: CVE-2017-9365**	https://github.com/bigtreecms/BigTree-CMS/commit/c17d09b05d9c20c214ee2f4fbb52f7307a7b4b6f	A-BIG-BIGTR-210617/29
CSRF	05-06-2017	6.8	BigTree CMS through 4.2.18 has CSRF related to the core\admin\modules\users\profile\update.php script (modify user information), the index.php/admin/developer/packages/delete/ URI (remove packages), the index.php/admin/developer/up	https://github.com/bigtreecms/BigTree-CMS/issues/293	A-BIG-BIGTR-210617/30

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

			grade/ignore/?versions= URI, and the index.php/admin/developer/upgrade/set-ftp-directory/ URI. **CVE ID: CVE-2017-9444**		
Execute Code Bypass	02-06-2017	7.5	Unrestricted File Upload exists in BigTree CMS through 4.2.18: if an attacker uploads an 'xxx.pht' or 'xxx.phtml' file, they could bypass a safety check and execute any code. **CVE ID: CVE-2017-9364**	https://github.com/bigtreecms/BigTree-CMS/commit/b7229394695 1cc650eaf51f5 d2f62ceac6335 e12	A-BIG-BIGTR-210617/31
Bluecoat					
Advanced Secure Gateway;Cacheflow;Proxysg					
Bypass	08-06-2017	5	Blue Coat Advanced Secure Gateway 6.6, CacheFlow 3.4, ProxySG 6.5 and 6.6 allows remote attackers to bypass blocked requests, user authentication, and payload scanning. **CVE ID: CVE-2016-6594**	https://bto.bluecoat.com/security-advisory/sa130	A-BLU-ADVAN-210617/32
Bluez					
Bluez					
Execute Code; Overflow	09-06-2017	4.6	Buffer overflow in BlueZ 5.41 and earlier allows an attacker to execute arbitrary code via the parse_line function used in some userland utilities. **CVE ID: CVE-2016-7837**	https://git.kernel.org/pub/scm/bluetooth/bluez.git/commit/?id=8514068 150759c1d6a4 6d4605d2351 babfde1601	A-BLU-BLUEZ-210617/33
Call-cc					
Chicken					
DoS; Bypass	01-06-2017	5	An incorrect "pair?" check in the Scheme "length" procedure results in an unsafe pointer dereference in all CHICKEN Scheme versions prior to 4.13, which allows an attacker to cause a denial of service by passing an improper list to an	http://lists.nongnu.org/archive/html/chicken-announce/2017-05/msg00000.html	A-CAL-CHICK-210617/34

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

			application that calls "length" on it. **CVE ID: CVE-2017-9334**		
Cgiirc					
CGI					
XSS	06-06-2017	4.3	irc.cgi in CGI:IRC before 0.5.12 reflects user-supplied input from the R parameter without proper output encoding, aka XSS. **CVE ID: CVE-2017-8920**	http://cgiirc.org/	A-CGI-CGI-210617/35
Cisco					
Anyconnect Secure Mobility Client					
Execute Code	08-06-2017	7.2	A vulnerability in how DLL files are loaded with Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to install and run an executable file with Gain Privilegesileges equivalent to the Microsoft Windows SYSTEM account. The vulnerability is due to incomplete input validation of path and file names of a DLL file before it is loaded. An attacker could exploit this vulnerability by creating a malicious DLL file and installing it in a specific system directory. A successful exploit could allow the attacker to execute commands on the underlying Microsoft Windows host with Gain Privilegesileges equivalent to the SYSTEM account. The attacker would need valid user credentials to exploit this vulnerability. This vulnerability affects all Cisco AnyConnect Secure Mobility Client for Windows software versions prior to 4.4.02034. Cisco Bug IDs: CSCvc97928. **CVE ID: CVE-2017-6638**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-anyconnect	A-CIS-ANYCO-210617/36

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

Elastic Services Controller					
NA	13-06-2017	6.5	A vulnerability in the ConfD CLI of Cisco Elastic Services Controllers could allow an authenticated, remote attacker to log in to an affected system as the admin user, aka an Insecure Default Administrator Credentials Vulnerability. More Information: CSCvc76661. Known Affected Releases: 2.2(9.76). **CVE ID: CVE-2017-6689**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-esc5	A-CIS-ELAST-210617/37
NA	13-06-2017	9	A vulnerability in Cisco Elastic Services Controllers could allow an authenticated, remote attacker to log in to an affected system as the Linux root user, aka an Insecure Default Password Vulnerability. More Information: CSCvc76631. Known Affected Releases: 2.2(9.76). **CVE ID: CVE-2017-6688**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-esc4	A-CIS-ELAST-210617/38
Email Security Appliance					
Bypass	13-06-2017	5	A vulnerability in the email message scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured filters on the device, as demonstrated by the Attachment Filter. More Information: CSCvd34632. Known Affected Releases: 10.0.1-087 9.7.1-066. Known Fixed Releases: 10.0.2-020 9.8.1-015. **CVE ID: CVE-2017-6671**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-esa1	A-CIS-EMAIL-210617/39
Firesight System					
Bypass	13-06-2017	5	A vulnerability in the feature-license management functionality of Cisco Firepower	https://tools.cisco.com/security/center/cont	A-CIS-FIRES-210617/

			System Software could allow an unauthenticated, remote attacker to bypass URL filters that have been configured for an affected device. More Information: CSCvb16413. Known Affected Releases: 6.0.1 6.1.0 6.2.0 6.2.1. Known Fixed Releases: 6.2.1 6.2.0.1 6.1.0.2. **CVE ID: CVE-2017-6674**	ent/CiscoSecurityAdvisory/cisco-sa-20170524-fmc	40
Industrial Network Director					
XSS	13-06-2017	4.3	Vulnerability in the web interface of Cisco Industrial Network Director could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against an affected system. More Information: CSCvd25405. Known Affected Releases: 1.1(0.176). **CVE ID: CVE-2017-6675**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-ind	A-CIS-INDUS-210617/41
Prime Data Center Network Manager					
Gain Privileges	08-06-2017	10	Vulnerability in Cisco Prime Data Center Network Manager (DCNM) Software could allow an unauthenticated, remote attacker to log in to the administrative console of a DCNM server by using an account that has a default, static password. The account could be granted root- or system-level Gain Privileges. The vulnerability exists because the affected software has a default user account that has a default, static password. The user account is created automatically when the software is installed. An attacker could exploit this vulnerability by connecting remotely to an affected system and logging in to the affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-dcnm2	A-CIS-PRIME-210617/42

			software by using the credentials for this default user account. A successful exploit could allow the attacker to use this default user account to log in to the affected software and gain access to the administrative console of a DCNM server. This vulnerability affects Cisco Prime Data Center Network Manager (DCNM) Software releases prior to Release 10.2(1) for Microsoft Windows, Linux, and Virtual Appliance platforms. Cisco Bug IDs: CSCvd95346. **CVE ID: CVE-2017-6640**		
Execute Code	08-06-2017	10	Vulnerability in the role-based access control (RBAC) functionality of Cisco Prime Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to access sensitive information or execute arbitrary code with root Gain Privilegesileges on an affected system. The vulnerability is due to the lack of authentication and authorization mechanisms for a debugging tool that was inadvertently enabled in the affected software. An attacker could exploit this vulnerability by remotely connecting to the debugging tool via TCP. A successful exploit could allow the attacker to access sensitive information about the affected software or execute arbitrary code with root Gain Privilegesileges on the affected system. This vulnerability affects Cisco Prime Data Center Network Manager (DCNM)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-dcnm1	A-CIS-PRIME-210617/43

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

			Software Releases 10.1(1) and 10.1(2) for Microsoft Windows, Linux, and Virtual Appliance platforms. Cisco Bug IDs: CSCvd09961. **CVE ID: CVE-2017-6639**		
Telepresence Ce Software; Telepresence Tc Software					
DoS	08-06-2017	7.8	Vulnerability in the Session Initiation Protocol (SIP) of the Cisco TelePresence Codec (TC) and Collaboration Endpoint (CE) Software could allow an unauthenticated, remote attacker to cause a TelePresence endpoint to reload unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to a lack of flow-control mechanisms within the software. An attacker could exploit this vulnerability by sending a flood of SIP INVITE packets to the affected device. An exploit could allow the attacker to impact the availability of services and data of the device, including a complete DoS condition. This vulnerability affects the following Cisco TC and CE platforms when running software versions prior to TC 7.3.8 and CE 8.3.0. Cisco Bug IDs: CSCux94002. **CVE ID: CVE-2017-6648**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-tele	A-CIS-TELEP-210617/44
Ultra Services Framework Element Manager					
NA	13-06-2017	6.5	A vulnerability in Cisco Ultra Services Framework Element Manager could allow an authenticated, remote attacker with access to the management network to log in to the affected device using default credentials present on the system, aka an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-usf5	A-CIS-ULTRA-210617/45

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

			Insecure Default Password Vulnerability. More Information: CSCvc76695. Known Affected Releases: 21.0.0. **CVE ID: CVE-2017-6687**		
NA	13-06-2017	6.5	A vulnerability in Cisco Ultra Services Framework Element Manager could allow an authenticated, remote attacker with access to the management network to log in as an admin or oper user of the affected device, aka an Insecure Default Credentials Vulnerability. More Information: CSCvc76699. Known Affected Releases: 21.0.0. **CVE ID: CVE-2017-6686**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-usf4	A-CIS-ULTRA-210617/46
NA	13-06-2017	9	A vulnerability in Cisco Ultra Services Framework Element Manager could allow an authenticated, remote attacker to log in to the device with the Gain Privilegesileges of the root user, aka an Insecure Default Account Information Vulnerability. More Information: CSCvd85710. Known Affected Releases: 21.0.v0.65839. **CVE ID: CVE-2017-6692**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-usf6	A-CIS-ULTRA-210617/47
Cisofy					
Lynis					
Gain Privileges	08-06-2017	4.6	Unspecified tests in Lynis before 2.5.0 allow local users to write to arbitrary files or possibly gain Gain Privileges via a symlink attack on a temporary file. **CVE ID: CVE-2017-8108**	https://github.com/CISOfy/lynis/releases/tag/2.5.0	A-CIS-LYNIS-210617/48
Cloud Foundry					
Diego					
DoS	08-06-2017	5	Cloud Foundry Diego 0.1468.0 through 0.1470.0 allows remote attackers to cause a denial of service.	http://www.openwall.com/lists/oss-security/2016	A-CLO-DIEGO-210617/49

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

			CVE ID: CVE-2016-3091	/05/17/8	
Codecabin					
Wp Live Chat Support					
XSS	09-06-2017	4.3	Cross-site scripting vulnerability in WP Live Chat Support prior to version 7.0.07 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE ID: CVE-2017-2187**	https://plugins.trac.wordpress.org/changeset/1658232/	A-COD-WP LI-210617/50
Cryptopp					
Crypto++					
NA	05-06-2017	5	Crypto++ (aka cryptopp) through 5.6.5 contains an out-of-bounds read vulnerability in zinflate.cpp in the Inflator filter. **CVE ID: CVE-2017-9434**	http://openwall.com/lists/oss-security/2017/06/06/2	A-CRY-CRYPT-210617/51
Cybozu					
Dezie					
Bypass Gain Information	09-06-2017	5	Cybozu Dezie 8.0.0 to 8.1.1 allows remote attackers to bypass access restrictions to obtain an arbitrary DBM (Cybozu Dezie proprietary format) file via unspecified vectors. **CVE ID: CVE-2016-7832**	https://support.cybozu.com/ja-jp/article/9742	A-CYB-DEZIE-210617/52
Bypass	09-06-2017	6.4	Cybozu Dezie 8.0.0 to 8.1.1 allows remote attackers to bypass access restrictions to delete an arbitrary DBM (Cybozu Dezie proprietary format) file via unspecified vectors. **CVE ID: CVE-2016-7833**	https://support.cybozu.com/ja-jp/article/9741	A-CYB-DEZIE-210617/53
Garoon					
CSRF	09-06-2017	4.3	Cross-site request forgery (CSRF) vulnerability in Cybozu Garoon 3.0.0 to 4.2.2 allows remote attackers to hijack the authentication of a logged in user to force a logout via unspecified vectors. **CVE ID: CVE-2016-4909**	https://support.cybozu.com/ja-jp/article/9459	A-CYB-GAROO-210617/54

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

XSS	09-06-2017	4.3	Cross-site scripting vulnerability in Cybozu Garoon 3.0.0 to 4.2.2 allows remote attackers to inject arbitrary web script or HTML via "Messages" function of Cybozu Garoon Keitai. **CVE ID: CVE-2016-4906**	https://support.cybozu.com/ja-jp/article/9511	A-CYB-GAROO-210617/55
Execute Code; Sql	09-06-2017	6.5	SQL injection vulnerability in the Cybozu Garoon 3.0.0 to 4.2.2 allows remote authenticated attackers to execute arbitrary SQL commands via "MultiReport" function. **CVE ID: CVE-2016-7803**	https://support.cybozu.com/ja-jp/article/9447	A-CYB-GAROO-210617/56
CSRF	09-06-2017	6.8	Cybozu Garoon 3.0.0 to 4.2.2 allow remote attackers to obtain CSRF tokens via unspecified vectors. **CVE ID: CVE-2016-4907**	https://support.cybozu.com/ja-jp/article/9441	A-CYB-GAROO-210617/57
Dest-unreach					
Socat					
DoS	08-06-2017	5	The signal handler implementations in socat before 1.7.3.0 and 2.0.0-b8 allow remote attackers to cause a denial of service (process freeze or crash). **CVE ID: CVE-2015-1379**	https://bugzilla.redhat.com/show_bug.cgi?id=1185711	A-DES-SOCAT-210617/58
Digium					
Certified Asterisk; Open Source					
DoS Overflow	02-06-2017	5	PJSIP, as used in Asterisk Open Source 13.x before 13.15.1 and 14.x before 14.4.1, Certified Asterisk 13.13 before 13.13-cert4, and other products, allows remote attackers to cause a denial of service (buffer overflow and application crash) via a SIP packet with a crafted CSeq header in conjunction with a Via header that lacks a branch parameter. **CVE ID: CVE-2017-9372**	http://downloads.asterisk.org/pub/security/AST-2017-002.txt	A-DIG-CERTI-210617/59

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	02-06-2017	5	The multi-part body parser in PJSIP, as used in Asterisk Open Source 13.x before 13.15.1 and 14.x before 14.4.1, Certified Asterisk 13.13 before 13.13-cert4, and other products, allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet. **CVE ID: CVE-2017-9359**	http://downloads.asterisk.org/pub/security/AST-2017-003.txt	A-DIG-CERTI-210617/60
Dnstracer Project					
Dnstracer					
DoS Overflow	05-06-2017	7.5	Stack-based buffer overflow in dnstracer through 1.9 allows attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a command line with a long name argument that is mishandled in a strcpy call for argv[0]. An example threat model is a web application that launches dnstracer with an untrusted name string. **CVE ID: CVE-2017-9430**	NA	A-DNS-DNSTR-210617/61
Dolibarr					
Dolibarr					
Sql	05-06-2017	7.5	Dolibarr ERP/CRM before 5.0.3 is vulnerable to a SQL injection in user/index.php (search_supervisor and search_statut parameters). **CVE ID: CVE-2017-9435**	https://github.com/Dolibarr/dolibarr/commit/70636cc59ffa1ffbc0ce3dba315d7d9b837aad04	A-DOL-DOLIB-210617/62
Elastic					
X-pack					
NA	05-06-2017	6.5	Elastic X-Pack Security versions 5.0.0 to 5.4.0 contain a Gain Privilegesilege escalation bug in the run_as functionality. This bug prevents transitioning into the specified user specified in a	https://discuss.elastic.co/t/elastic-stack-5-4-1-and-5-3-3-security-updates/8795	A-ELA-X-PAC-210617/63

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

			run_as request. If a role has been created using a template that contains the _user properties, the behavior of run_as will be incorrect. Additionally if the run_as user specified does not exist, the transition will not happen. **CVE ID: CVE-2017-8438**	2	
Elasticsearch					
Kibana					
XSS; Gain Information	05-06-2017	4.3	Starting in version 5.3.0, Kibana had a cross-site scripting (XSS) vulnerability in the Discover page that could allow an attacker to obtain sensitive information from or perform destructive actions on behalf of other Kibana users. **CVE ID: CVE-2017-8440**	https://www.elastic.co/community/security	A-ELA-KIBAN-210617/64
XSS; Gain Information	05-06-2017	4.3	Kibana version 5.4.0 was affected by a Cross Site Scripting (XSS) bug in the Time Series Visual Builder. This bug could allow an attacker to obtain sensitive information from Kibana users. **CVE ID: CVE-2017-8439**	https://www.elastic.co/community/security	A-ELA-KIBAN-210617/65
Emon-cms					
Deraemon-cms					
XSS	09-06-2017	4.3	Cross-site scripting vulnerability in DERAEMON-CMS version 0.8.9 and earlier allows remote attackers to inject arbitrary web script or HTML via the parameters hostname, database and username. **CVE ID: CVE-2016-7813**	http://emon-cms.com/new11	A-EMO-DERAE-210617/66
Event List Project					
Event List					
Execute Code Sql	13-06-2017	6.5	SQL injection vulnerability in the Event List plugin 0.7.8 for WordPress allows an	http://dtsa.eu/CVE ID: CVE-2017-9429-	A-EVE-EVENT-210617/

			authenticated user to execute arbitrary SQL commands via the id parameter to wp-admin/admin.php. **CVE ID: CVE-2017-9429**	event-list-version-v-0-7-8-blind-based-sql-injection-sqli/	67
Fenrir-inc					
Sleipnir					
NA	09-06-2017	5.8	Sleipnir 4 Black Edition for Mac 4.5.3 and earlier and Sleipnir 4 for Mac 4.5.3 and earlier (Mac App Store) may allow a remote attacker to spoof the URL display via a specially crafted webpage. **CVE ID: CVE-2016-7831**	NA	A-FEN-SLEIP-210617/68
File-path Project					
File-path Module					
NA	01-06-2017	4.3	Race condition in the rmtree and remove_tree functions in the File-Path module before 2.13 for Perl allows attackers to set the mode on arbitrary files via vectors involving directory-permission loosening logic. **CVE ID: CVE-2017-6512**	http://cpansearch.perl.org/src/JKEENAN/File-Path-2.13/Changes	A-FIL-FILE--210617/69
Flatcore					
Flatcore					
XSS	06-06-2017	4.3	Cross site scripting (XSS) vulnerability in pages.edit_form.php in flatCore 1.4.6 allows remote attackers to inject arbitrary JavaScript via the PATH_INFO in an acp.php URL, due to use of unsanitized $_SERVER['PHP_SELF'] to generate URLs. **CVE ID: CVE-2017-9451**	https://github.com/flatCore/flatCore-CMS/commit/f1b42b338693a9c240182e76ef2131057f2c2a87	A-FLA-FLATC-210617/70
Flipbuilder					
Flip Pdf					
XSS	01-06-2017	4.3	Cross-site scripting (XSS) vulnerability in FlipBuilder Flip PDF allows remote attackers to inject arbitrary web script or	https://bits3c.blogspot.dk/2017/05/CVE-2017-7384-	A-FLI-FLIP - 210617/71

			HTML via the currentHTMLURL parameter. **CVE ID: CVE-2017-7384**	reflected-xss-in-flippdf.html	
Freedesktop					
Poppler					
DoS; Overflow	02-06-2017	4.3	In Poppler 0.54.0, a memory leak vulnerability was found in the function Object::initArray in Object.cc, which allows attackers to cause a denial of service via a crafted file. **CVE ID: CVE-2017-9408**	https://bugs.freedesktop.org/show_bug.cgi?id=100776	A-FRE-POPPL-210617/72
DoS; Overflow	02-06-2017	4.3	In Poppler 0.54.0, a memory leak vulnerability was found in the function gmalloc in gmem.cc, which allows attackers to cause a denial of service via a crafted file. **CVE ID: CVE-2017-9406**	https://bugs.freedesktop.org/show_bug.cgi?id=100775	A-FRE-POPPL-210617/73
NA	06-06-2017	4.3	poppler through version 0.55.0 is vulnerable to an uncontrolled recursion in pdfunite resulting into potential denial-of-service. **CVE ID: CVE-2017-7515**	https://bugs.freedesktop.org/show_bug.cgi?id=101208	A-FRE-POPPL-210617/74
Gnome					
Libcroco					
DoS Overflow	12-06-2017	4.3	The cr_tknzr_parse_comment function in cr-tknzr.c in libcroco 0.6.12 allows remote attackers to cause a denial of service (memory allocation error) via a crafted CSS file. **CVE ID: CVE-2017-8834**	NA	A-GNO-LIBCR-210617/75
DoS	12-06-2017	7.1	The cr_parser_parse_selector_core function in cr-parser.c in libcroco 0.6.12 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted CSS file. **CVE ID: CVE-2017-8871**	NA	A-GNO-LIBCR-210617/76
GNU					

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

Glibc					
Execute Code Overflow	12-06-2017	7.5	nscd in the GNU C Library (aka glibc or libc6) before version 2.20 does not correctly compute the size of an internal buffer when processing netgroup requests, possibly leading to an nscd daemon crash or code execution as the user running nscd. **CVE ID: CVE-2014-9984**	https://sourceware.org/bugzilla/show_bug.cgi?id=16695	A-GNU-GLIBC-210617/77
Libssp					
Overflow	07-06-2017	4.6	Binaries compiled against targets that use the libssp library in GCC for stack smashing protection (SSP) might allow local users to perform buffer overflow attacks by leveraging lack of the Object Size Checking feature. **CVE ID: CVE-2016-4973**	https://bugzilla.redhat.com/show_bug.cgi?id=1324759	A-GNU-LIBSS-210617/78
Goldplugins					
Testimonials Plugin Easy Testimonials					
Execute Code; Sql	12-06-2017	6.5	SQL injection vulnerability in the WP-Testimonials plugin 3.4.1 for WordPress allows an authenticated user to execute arbitrary SQL commands via the testid parameter to wp-admin/admin.php. **CVE ID: CVE-2017-9418**	http://dtsa.eu/wp-testimonials-wordpress-plugin-v-3-4-1-union-based-sql-injection-sqli/	A-GOL-TESTI-210617/79
Google					
Chrome					
DoS; Memory Corruption	06-06-2017	4.3	Double-free vulnerability in libavformat/mov.c in FFMPEG in Google Chrome 41.0.2251.0 allows remote attackers to cause a denial of service (memory corruption and crash) via a crafted .m4a file. **CVE ID: CVE-2015-1207**	https://gist.github.com/bittorrent3389/8fee7cdaa73d1d351ee9	A-GOO-CHROM-210617/80
Grpc					
Grpc					

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

Overflow	04-06-2017	7.5	Google gRPC before 2017-04-05 has an out-of-bounds write caused by a heap-based buffer overflow related to core/lib/iomgr/error.c. **CVE ID: CVE-2017-9431**	NA	A-GRP-GRPC-210617/81
H2O Project					
H2O					
Gain Information	09-06-2017	6.4	Use-after-free vulnerability in H2O allows remote attackers to cause a denial-of-service (DoS) or obtain server certificate Gain Privilegesate keys and possibly other information. **CVE ID: CVE-2016-7835**	https://github.com/h2o/h2o/issues/1144	A-H2O-H2O-210617/82
IBM					
Bigfix Security Compliance Analytics					
XSS	07-06-2017	4.3	IBM Endpoint Manager for Security and Compliance 1.9.70 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 123430. **CVE ID: CVE-2017-1178**	http://www.ibm.com/support/docview.wss?uid=swg22004164	A-IBM-BIGFI-210617/83
NA	08-06-2017	4.3	IBM BigFix Compliance Analytics 1.9.79 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 123431. **CVE ID: CVE-2017-1179**	http://www.ibm.com/support/docview.wss?uid=swg22004161	A-IBM-BIGFI-210617/84
NA	07-06-2017	5	IBM BigFix Compliance (TEMA SUAv1 SCA SCM) 1.9.70 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user	http://www.ibm.com/support/docview.wss?uid=swg22004168	A-IBM-BIGFI-210617/85

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

			accounts. IBM X-Force ID: 123671. **CVE ID: CVE-2017-1196**		
Cognos Business Intelligence					
DoS	07-06-2017	6.8	IBM Cognos Business Intelligence 10.1 and 10.2 is vulnerable to a denial of service, caused by an XML External Entity Injection (XXE) error when processing XML data. A remote authenticated attacker could exploit this vulnerability to consume all available CPU resources and cause a denial of service. IBM X-Force ID: 110563. **CVE ID: CVE-2016-0254**	http://www.ibm.com/support/docview.wss?uid=swg22004036	A-IBM-COGNO-210617/86
Cognos Business Intelligence Server					
Gain Information	07-06-2017	5	IBM Predictive Solutions Foundation (formerly PMQ) could allow a remote attacker to include arbitrary files. A remote attacker could send a specially-crafted URL to specify a file from the local system, which could allow the attacker to obtain sensitive information. IBM X-Force ID: 119618. **CVE ID: CVE-2016-9710**	http://www.ibm.com/support/docview.wss?uid=swg22004036	A-IBM-COGNO-210617/87
Curam Social Program Management					
Gain Information	08-06-2017	5	Curam Universal Access in IBM Curam Social Program Management (SPM) 6.0 SP2 before EP26, 6.0.4 before 6.0.4.6, and 6.0.5 before 6.0.5.5 iFix5 allows remote attackers to obtain sensitive information about internal caseworker usernames via vectors related to a URL. **CVE ID: CVE-2014-4843**	http://www-01.ibm.com/support/docview.wss?uid=swg21698548	A-IBM-CURAM-210617/88
Domino					
NA	07-06-2017	5	IBM Domino 8.5 and 9.0 could allow an attacker to steal	http://www.ibm.com/suppor	A-IBM-DOMIN-

			credentials using multiple sessions and large amounts of data using Domino TLS Key Exchange validation. IBM X-Force ID: 117918. **CVE ID: CVE-2016-6087**	t/docview.wss?uid=swg22002808	210617/89
Maximo Asset Management					
Execute Code	13-06-2017	6.5	IBM Maximo Asset Management 7.5 and 7.6 could allow a remote authenticated attacker to execute arbitrary commands on the system as administrator. IBM X-Force ID: 120276. **CVE ID: CVE-2016-9984**	http://www.ibm.com/support/docview.wss?uid=swg21998608	A-IBM-MAXIM-210617/90
Maximo Asset Management;Maximo Asset Management Essentials					
NA	07-06-2017	6.5	IBM Maximo Asset Management 7.1, 7.5, and 7.6 could allow a remote attacker to hijack a user's session, caused by the failure to invalidate an existing session identifier. An attacker could exploit this vulnerability to gain access to another user's session. IBM X-Force ID: 120253. **CVE ID: CVE-2016-9977**	http://www.ibm.com/support/docview.wss?uid=swg22003981	A-IBM-MAXIM-210617/91
Rational Rhapsody Design Manager					
DoS	08-06-2017	7.5	IBM Rhapsody DM 4.0, 5.0, and 6.0 is vulnerable to a denial of service, caused by an XML External Entity Injection (XXE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume all available memory resources. IBM Reference #: 1999960. **CVE ID: CVE-2016-9698**	http://www.ibm.com/support/docview.wss?uid=swg22002258	A-IBM-RATIO-210617/92
Security Key Lifecycle Manager; Tivoli Key Lifecycle Manager					
NA	08-06-2017	5	IBM Tivoli Key Lifecycle Manager does not require that users should have strong passwords by default, which	http://www.ibm.com/support/docview.wss?uid=swg2199	A-IBM-SECUR-210617/93

			makes it easier for attackers to compromise user accounts. **CVE ID: CVE-2016-6093**	7956	
NA	08-06-2017	5.5	IBM Tivoli Key Lifecycle Manager 2.0.1, 2.5, and 2.6 specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors. **CVE ID: CVE-2016-6098**	http://www.ibm.com/support/docview.wss?uid=swg21997958	A-IBM-SECUR-210617/94
Security Gain Privileges Identity Manager					
Gain Information	07-06-2017	5	IBM Security Gain Privileges Identity Manager 2.0.2 and 2.1.0 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 116136. **CVE ID: CVE-2016-5959**	http://www.ibm.com/support/docview.wss?uid=swg22003092	A-IBM-SECUR-210617/95
Sterling Selling And Fulfillment Foundation					
CSRF	08-06-2017	6	IBM Sterling Order Management 9.2 through 9.5 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 121314. **CVE ID: CVE-2016-9991**	http://www-01.ibm.com/support/docview.wss?uid=swg21998167	A-IBM-STERL-210617/96
Tivoli Federated Identity Manager					
NA	08-06-2017	5	IBM Tivoli Federated Identity Manager 6.2 is affected by a vulnerability due to a missing secure attribute in encrypted session (SSL) cookie. IBM X-Force ID: 125731. **CVE ID: CVE-2017-1319**	http://www-01.ibm.com/support/docview.wss?uid=swg22002871	A-IBM-TIVOL-210617/97
Websphere Application Server					
Gain	08-06-2017	5	IBM WebSphere Application	http://www.ib	A-IBM-

Information			Server using malformed SOAP requests could allow a remote attacker to obtain sensitive information. **CVE ID: CVE-2016-9736**	m.com/support/docview.wss?uid=swg21996820	WEBSP-210617/98
Igcb					
Intellect Digital Core					
XSS	07-06-2017	4.3	Cross-site scripting (XSS) vulnerability in Intellect Design Arena Intellect Core banking software. **CVE ID: CVE-2015-6540**	NA	A-IGC-INTEL-210617/99
Imagemagick					
Imagemagick					
DoS Overflow	02-06-2017	4.3	In ImageMagick 7.0.5-5, the ReadMPCImage function in mpc.c allows attackers to cause a denial of service (memory leak) via a crafted file. **CVE ID: CVE-2017-9409**	https://github.com/ImageMagick/ImageMagick/issues/458	A-IMA-IMAGE-210617/
DoS Overflow	02-06-2017	4.3	In ImageMagick 7.0.5-5, the ReadPALMImage function in palm.c allows attackers to cause a denial of service (memory leak) via a crafted file. **CVE ID: CVE-2017-9407**	https://github.com/ImageMagick/ImageMagick/issues/459	A-IMA-IMAGE-210617/100
DoS Overflow	02-06-2017	4.3	In ImageMagick 7.0.5-5, the ReadICONImage function in icon.c:452 allows attackers to cause a denial of service (memory leak) via a crafted file. **CVE ID: CVE-2017-9405**	https://github.com/ImageMagick/ImageMagick/issues/457	A-IMA-IMAGE-210617/101
DoS Overflow	05-06-2017	4.3	In ImageMagick 7.0.5-5, a memory leak was found in the function ReadPSDChannel in coders/psd.c, which allows attackers to cause a denial of service via a crafted file. **CVE ID: CVE-2017-9440**	https://github.com/ImageMagick/ImageMagick/issues/462	A-IMA-IMAGE-210617/102
DoS Overflow	05-06-2017	4.3	In ImageMagick 7.0.5-5, a memory leak was found in the function ReadPDBImage in coders/pdb.c, which allows	https://github.com/ImageMagick/ImageMagick/issues/46	A-IMA-IMAGE-210617/103

			attackers to cause a denial of service via a crafted file. **CVE ID: CVE-2017-9439**	0	
DoS	07-06-2017	4.3	In ImageMagick 7.0.5-7 Q16, an assertion failure was found in the function LockSemaphoreInfo, which allows attackers to cause a denial of service via a crafted file. **CVE ID: CVE-2017-9501**	https://github.com/ImageMagick/ImageMagick/commit/01843366d6a7b96e22ad7bb67f3df7d9fd4d5d74	A-IMA-IMAGE-210617/104
DoS	07-06-2017	4.3	In ImageMagick 7.0.5-8 Q16, an assertion failure was found in the function ResetImageProfileIterator, which allows attackers to cause a denial of service via a crafted file. **CVE ID: CVE-2017-9500**	https://github.com/ImageMagick/ImageMagick/issues/500	A-IMA-IMAGE-210617/105
DoS	07-06-2017	4.3	In ImageMagick 7.0.5-7 Q16, an assertion failure was found in the function SetPixelChannelAttributes, which allows attackers to cause a denial of service via a crafted file. **CVE ID: CVE-2017-9499**	https://github.com/ImageMagick/ImageMagick/commit/7fd419441bc7103398e313558171d342c6315f44	A-IMA-IMAGE-210617/106
Intensewp					
Wp Jobs					
Execute Code; Sql	13-06-2017	6.5	SQL injection vulnerability in the WP Jobs plugin before 1.5 for WordPress allows authenticated users to execute arbitrary SQL commands via the jobid parameter to wp-admin/edit.php. **CVE ID: CVE-2017-9603**	NA	A-INT-WP JO-210617/107
IPA					
Appgoat					
Gain Information	09-06-2017	4.3	Hands-on Vulnerability Learning Tool "AppGoat" for Web Application V3.0.2 and earlier allow remote attackers to obtain	http://jvn.jp/en/jp/JVN32120290/index.html	A-IPA-APPGO-210617/108

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

			local files via unspecified vectors. **CVE ID: CVE-2017-2180**		
NA	09-06-2017	6.8	Hands-on Vulnerability Learning Tool "AppGoat" for Web Application V3.0.2 and earlier allow remote attackers to obtain local files via unspecified vectors, a different vulnerability than CVE-2017-2179 and CVE-2017-2181. **CVE ID: CVE-2017-2182**	http://jvn.jp/en/jp/JVN01404851/index.html	A-IPA-APPGO-210617/109
NA	09-06-2017	6.8	Hands-on Vulnerability Learning Tool "AppGoat" for Web Application V3.0.2 and earlier allow remote attackers to obtain local files via unspecified vectors, a different vulnerability than CVE-2017-2179 and: CVE-2017-2182. **CVE ID: CVE-2017-2181**	http://jvn.jp/en/jp/JVN20870477/index.html	A-IPA-APPGO-210617/110
Execute Code	09-06-2017	6.8	Hands-on Vulnerability Learning Tool "AppGoat" for Web Application V3.0.2 and earlier allows remote code execution via unspecified vectors, a different vulnerability than CVE-2017-2181 and: CVE-2017-2182. **CVE ID: CVE-2017-2179**	http://jvn.jp/en/jp/JVN80238098/index.html	A-IPA-APPGO-210617/111
Irssi					
Irssi					
Overflow	06-06-2017	5	In Irssi before 1.0.3, when receiving certain incorrectly quoted DCC files, it tries to find the terminating quote one byte before the allocated memory. Thus, remote attackers might be able to cause a crash. **CVE ID: CVE-2017-9469**	https://irssi.org/security/irssi_sa_2017_06.txt	A-IRS-IRSSI-210617/112
NA	06-06-2017	5	In Irssi before 1.0.3, when receiving a DCC message without source nick/host, it attempts to dereference a NULL	https://irssi.org/security/irssi_sa_2017_06.txt	A-IRS-IRSSI-210617/113

			pointer. Thus, remote IRC servers can cause a crash. **CVE ID: CVE-2017-9468**		
Jamroom					
Jamroom					
XSS	04-06-2017	4.3	Cross Site Scripting (XSS) exists in Jamroom before 4.2.7 via the Status Update field. **CVE ID: CVE-2012-6705**	NA	A-JAM-JAMRO-210617/114
Lenovo					
Active Protection System					
DoS	04-06-2017	4.9	In Lenovo Active Protection System before 1.82.0.14, an attacker with local Gain Privileges could send commands to the system's embedded controller, which could cause a denial of service attack on the system or the ability to alter hardware functionality. **CVE ID: CVE-2017-3740**	https://support.lenovo.com/us/en/product_security/LEN-13637	A-LEN-ACTIV-210617/115
Lenovo Service Bridge					
NA	04-06-2017	5	In Lenovo Service Bridge before version 4, a bug found in the signature verification logic of the code signing certificate could be exploited by an attacker to insert a forged code signing certificate. **CVE ID: CVE-2016-8231**	https://support.lenovo.com/us/en/product_security/LEN-10149	A-LEN-LENOV-210617/116
info	04-06-2017	5	In Lenovo Service Bridge before version 4, an insecure HTTP connection is used by LSB to send system serial number, machine type and model and product name to Lenovo's servers. **CVE ID: CVE-2016-8230**	https://support.lenovo.com/us/en/product_security/LEN-10149	A-LEN-LENOV-210617/117
CSRF	04-06-2017	6.8	A cross-site request forgery vulnerability in Lenovo Service Bridge before version 4 could be exploited by an attacker with access to the DHCP server used by the system where LSB is	https://support.lenovo.com/us/en/product_security/LEN-10149	A-LEN-LENOV-210617/118

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

			installed. **CVE ID: CVE-2016-8229**		
Execute Code	04-06-2017	7.2	In Lenovo Service Bridge before version 4, a user with local Gain Privilegesileges on a system could execute code with administrative Gain Privilegesileges. **CVE ID: CVE-2016-8228**	https://support.lenovo.com/us/en/product_security/LEN-10149	A-LEN-LENOV-210617/119
Libdwarf Project					
Libdwarf					
DoS	07-06-2017	4.3	dwarf_leb.c in libdwarf allows attackers to cause a denial of service (SIGSEGV). **CVE ID: CVE-2015-8538**	https://bugzilla.redhat.com/show_bug.cgi?id=1291299	A-LIB-LIBDW-210617/120
Libmwaw Project					
Libmwaw					
Overflow	04-06-2017	7.5	Document Liberation Project libmwaw before 2017-04-08 has an out-of-bounds write caused by a heap-based buffer overflow related to the MsWrd1Parser::readFootnoteCorrespondance function in lib/MsWrd1Parser.cxx. **CVE ID: CVE-2017-9433**	NA	A-LIB-LIBMW-210617/121
Libquicktime					
Libquicktime					
DoS; Overflow	12-06-2017	4.3	The quicktime_video_width function in lqt_quicktime.c in libquicktime 1.2.4 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted mp4 file. **CVE ID: CVE-2017-9128**	https://www.exploit-db.com/exploits/42148/	A-LIB-LIBQU-210617/122
DoS Overflow	12-06-2017	4.3	The quicktime_user_atoms_read_atom function in useratoms.c in libquicktime 1.2.4 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash)	https://www.exploit-db.com/exploits/42148/	A-LIB-LIBQU-210617/123

			via a crafted mp4 file. **CVE ID: CVE-2017-9127**		
DoS Overflow	12-06-2017	4.3	The quicktime_read_dref_table function in dref.c in libquicktime 1.2.4 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) via a crafted mp4 file. **CVE ID: CVE-2017-9126**	https://www.exploit-db.com/exploits/42148/	A-LIB-LIBQU-210617/124
DoS Overflow	12-06-2017	4.3	The lqt_frame_duration function in lqt_quicktime.c in libquicktime 1.2.4 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted mp4 file. **CVE ID: CVE-2017-9125**	https://www.exploit-db.com/exploits/42148/	A-LIB-LIBQU-210617/125
DoS	12-06-2017	4.3	The quicktime_match_32 function in util.c in libquicktime 1.2.4 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted mp4 file. **CVE ID: CVE-2017-9124**	https://www.exploit-db.com/exploits/42148/	A-LIB-LIBQU-210617/126
DoS	12-06-2017	4.3	The lqt_frame_duration function in lqt_quicktime.c in libquicktime 1.2.4 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted mp4 file. **CVE ID: CVE-2017-9123**	https://www.exploit-db.com/exploits/42148/	A-LIB-LIBQU-210617/127
DoS	12-06-2017	7.1	The quicktime_read_moov function in moov.c in libquicktime 1.2.4 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted mp4 file. **CVE ID: CVE-2017-9122**	https://www.exploit-db.com/exploits/42148/	A-LIB-LIBQU-210617/128
Libsndfile Project					
Libsndfile					

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

Overflow	12-06-2017	6.8	In libsndfile version 1.0.28, an error in the "aiff_read_chanmap()" function (aiff.c) can be exploited to cause an out-of-bounds read memory access via a specially crafted AIFF file. **CVE ID: CVE-2017-6892**	https://github.com/erikd/libsndfile/commit/f833c53cb596e9e1792949f762e0b33661822748	A-LIB-LIBSN-210617/129
Libstaroffice Project					
Libstaroffice					
Overflow	04-06-2017	7.5	Document Liberation Project libstaroffice before 2017-04-07 has an out-of-bounds write caused by a stack-based buffer overflow related to the DatabaseName::read function in lib/StarWriterStruct.cxx. **CVE ID: CVE-2017-9432**	NA	A-LIB-LIBST-210617/130
Libtiff					
Libtiff					
DoS; Overflow	02-06-2017	4.3	In LibTIFF 4.0.7, a memory leak vulnerability was found in the function OJPEGReadHeaderInfoSecTablesQTable in tif_ojpeg.c, which allows attackers to cause a denial of service via a crafted file. **CVE ID: CVE-2017-9404**	http://bugzilla.maptools.org/show_bug.cgi?id=2688	A-LIB-LIBTI-210617/131
DoS; Overflow	02-06-2017	4.3	In LibTIFF 4.0.7, a memory leak vulnerability was found in the function TIFFReadDirEntryLong8Array in tif_dirread.c, which allows attackers to cause a denial of service via a crafted file. **CVE ID: CVE-2017-9403**	http://bugzilla.maptools.org/show_bug.cgi?id=2689	A-LIB-LIBTI-210617/132
Markdown On Save Improved Project					
Markdown On Save Improved					
XSS	01-06-2017	4.3	The Markdown on Save Improved plugin 2.5 for WordPress has a stored XSS vulnerability in the content of a post.	http://lncken.cn/?p=279	A-MAR-MARKD-210617/133

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

			CVE ID: CVE-2017-9337		
Markdown-it Project					
Markdown-it					
NA	07-06-2017	5	markdown-it before 4.1.0 does not block data: URLs. **CVE ID: CVE-2015-3295**	https://github.com/markdown-it/markdown-it/commit/f76d3beb46abd121892a2e2e5c78376354c214e3	A-MAR-MARKD-210617/134
Mercurial					
Mercurial					
Execute Code	06-06-2017	9	In Mercurial before 4.1.3, "hg serve --stdio" allows remote authenticated users to launch the Python debugger, and consequently execute arbitrary code, by using --debugger as a repository name. **CVE ID: CVE-2017-9462**	https://bugs.debian.org/861243	A-MER-MERCU-210617/135
Microsoft					
Excel;Office					
Execute Code	14-06-2017	9.3	A remote code execution vulnerability exists in Microsoft Office when the software fails to properly handle objects in memory, aka "Office Remote Code Execution Vulnerability". This CVE ID is unique from CVE-2017-8509, CVE-2017-8511, CVE-2017-8512, CVE-2017-0260, and CVE-2017-8506. **CVE ID: CVE-2017-8510**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8510	A-MIC-EXCEL-210617/136
Office;Office Compatibility Pack;Office Web Apps;Office Web Apps Server;Onenote;Sharepoint Server;Word;Word For Mac					
Execute Code	14-06-2017	9.3	A remote code execution vulnerability exists in Microsoft Office when the software fails to properly handle objects in memory, aka "Office Remote Code Execution Vulnerability". This	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	A-MIC-OFFIC-210617/137

			CVE ID is unique fromCVE-2017-8510, CVE-2017-8511, CVE-2017-8512, CVE-2017-0260, and CVE-2017-8506. **CVE ID: CVE-2017-8509**	2017-8509	
Office; Office Online Server; Office Web Apps; Office Web Apps Server; Powerpoint For Mac; Sharepoint Server					
Execute Code	14-06-2017	9.3	A remote code execution vulnerability exists in Microsoft Office when the software fails to properly handle objects in memory, aka "Office Remote Code Execution Vulnerability". This CVE ID is unique from CVE-2017-8509, CVE-2017-8510, CVE-2017-8511, CVE-2017-0260, and CVE-2017-8506. **CVE ID: CVE-2017-8512**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8512	A-MIC-OFFIC-210617/138
Milton					
Webdav					
NA	07-06-2017	7.5	XML External Entity (XXE) vulnerability in Milton Webdav before 2.7.0.3. **CVE ID: CVE-2015-7326**	https://github.com/miltonio/milton2/commit/b5851c1	A-MIL-WEBDA-210617/139
Multi Feed Reader Project					
Multi Feed Reader					
Execute Code; Sql	09-06-2017	6.5	SQL injection vulnerability in the Multi Feed Reader prior to version 2.2.4 allows authenticated attackers to execute arbitrary SQL commands via unspecified vectors. **CVE ID: CVE-2017-2195**	https://wordpress.org/plugins/multi-feed-reader/#developers	A-MUL-MULTI-210617/140
Opa-ff Project;Opa-fm Project					
Opa-ff/Opa-fm					
NA	07-06-2017	9.3	Race conditions in opa-fm before 10.4.0.0.196 and opa-ff before 10.4.0.0.197. **CVE ID: CVE-2015-5232**	https://github.com/01org/opa-fm/commit/c5759e7b76f5bf844be6c6641cc1b356bb	A-OPA-OPA-F-210617/141

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

				c83869	
Openbravo					
Openbravo Erp					
Sql	05-06-2017	6.5	Openbravo Business Suite 3.0 is affected by SQL injection. This vulnerability could allow remote authenticated attackers to inject arbitrary SQL code. **CVE ID: CVE-2017-9437**	https://www.wizlynxgroup.com/security-research-advisories/vuln/WLX-2017-005	A-OPE-OPENB-210617/142
Open-emr					
Openemr					
Execute Code	02-06-2017	6.5	OpenEMR 5.0.0 and prior allows low-Gain Privileges users to upload files of dangerous types which can result in arbitrary code execution within the context of the vulnerable application. **CVE ID: CVE-2017-9380**	https://www.wizlynxgroup.com/security-research-advisories/vuln/WLX-2017-002	A-OPE-OPENE-210617/143
Open-xchange					
Open-xchange Appsuite;Open-xchange Server					
XSS	08-06-2017	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Open-Xchange Server 6 and OX AppSuite before 7.4.2-rev43, 7.6.0-rev38, and 7.6.1-rev21. **CVE ID: CVE-2015-1588**	NA	A-OPE-OPEN--210617/144
Personify					
Personify360 E-business					
NA	07-06-2017	5	An issue was discovered in Personify360 e-Business 7.5.2 through 7.6.1. When going to the /TabId/275 URI, while creating a new role, a list of database tables and their columns is available. **CVE ID: CVE-2017-7314**	https://amswoes.wordpress.com/2017/06/06/CVE-2017-7314-dump-personify-database-schema-33/	A-PER-PERSO-210617/145
Gain Information	07-06-2017	5	An issue was discovered in Personify360 e-Business 7.5.2 through 7.6.1. When going to the /TabId/275 URI, it is possible to read any customer name, master	https://amswoes.wordpress.com/2017/06/06/CVE-2017-7313-	A-PER-PERSO-210617/146

			Customer Id, and email address. In other words, anyone can search for users/customers in the system - no authentication is required. **CVE ID: CVE-2017-7313**	how-to-dump-personify-customer-data-with-one-click-23/	
NA	07-06-2017	7.5	An issue was discovered in Personify360 e-Business 7.5.2 through 7.6.1. When going to the /TabId/275 URI, anyone can add a vendor account or read existing vendor account data (including usernames and passwords). **CVE ID: CVE-2017-7312**	https://amswoes.wordpress.com/2017/06/06/first-blog-post/	A-PER-PERSO-210617/147
Pivotx					
Pivotx					
XSS	06-06-2017	4.3	The smarty_self function in modules/module_smarty.php in PivotX 2.3.11 mishandles the URI, allowing XSS via vectors involving quotes in the self Smarty tag. **CVE ID: CVE-2017-9332**	https://sourceforge.net/p/pivot-weblog/code/4487/	A-PIV-PIVOT-210617/148
Piwigo					
Piwigo					
NA	14-06-2017	5.8	An open redirect vulnerability is present in Piwigo 2.9 and probably prior versions, allowing remote attackers to redirect users to arbitrary web sites and conduct phishing attacks. The identification.php component is affected by this issue: the "redirect" parameter is not validated. **CVE ID: CVE-2017-9464**	NA	A-PIW-PIWIG-210617/149
Postgresql					
Postgresql					
NA	06-06-2017	5	PostgreSQL PL/Java after 9.0 does not honor access controls on large objects. **CVE ID: CVE-2016-0768**	https://tada.github.io/pljava/releasenotes.html	A-POS-POSTG-210617/150
Pulpproject					
Pulp					

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	08-06-2017	5	client/consumer/cli.py in Pulp before 2.8.3 writes consumer Gain Privilegesate keys to etc/pki/pulp/consumer/consumer-cert.pem as world-readable. **CVE ID: CVE-2016-3112**	https://pulp.plan.io/issues/1834	A-PUL-PULP-210617/151
Qemu					
Qemu					
DoS	01-06-2017	4.9	Memory leak in the virtio_gpu_set_scanout function in hw/display/virtio-gpu.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (memory consumption) via a large number of "VIRTIO_GPU_CMD_SET_SCANOUT:" commands. **CVE ID: CVE-2017-9060**	http://git.qemu.org/?p=qemu.git;a=commit;h=dd248ed7e204ee8a1873914e02b8b526e8f1b80d	A-QEM-QEMU-210617/152
Radare Project					
Radare2					
DoS	08-06-2017	4.3	The r_config_set function in libr/config/config.c in radare2 1.5.0 allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted DEX file. **CVE ID: CVE-2017-9520**	https://github.com/radare/radare2/commit/f85bc674b2a2256a364fe796351bc1971e106005	A-RAD-RADAR-210617/153
Rapid7					
Nexpose					
NA	06-06-2017	6.8	The default SSH configuration in Rapid7 Nexpose hardware appliances shipped before June 2017 does not specify desired algorithms for key exchange and other important functions. As a result, it falls back to allowing ALL algorithms supported by the relevant version of OpenSSH and makes the installations vulnerable to a range of MITM, downgrade, and decryption attacks.	https://community.rapid7.com/community/nexpose/blog/2017/05/31/r7-2017-13-nexpose-hardware-appliance-ssh-enabled-obsolete-algorithms-CVE-2017-	A-RAP-NEXPO-210617/154

			CVE ID: CVE-2017-5243	5243	
Rarlab					
RAR					
Directory Traversal	04-06-2017	4.3	Directory Traversal exists in RAR 4.x and 5.x because an unpack operation follows any symlinks, including symlinks contained in the archive. This allows remote attackers to write to arbitrary files via a crafted archive. **CVE ID: CVE-2014-9983**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=774172	A-RAR-RAR-210617/155
Redhat					
Cloudforms					
Execute Code	08-06-2017	6.5	ManageIQ in CloudForms before 4.1 allows remote authenticated users to execute arbitrary code. **CVE ID: CVE-2016-4471**	https://bugzilla.redhat.com/show_bug.cgi?id=1340763	A-RED-CLOUD-210617/156
Cloudforms Management Engine					
NA	08-06-2017	5	CloudForms Management Engine before 5.8 includes a default SSL/TLS certificate. **CVE ID: CVE-2016-4457**	https://bugzilla.redhat.com/show_bug.cgi?id=1341308	A-RED-CLOUD-210617/157
Satellite					
NA	07-06-2017	6.5	Red Hat Satellite 6 allows remote authenticated users with Gain Privileges access on a content host to authenticate to the capsule broker or server broker. **CVE ID: CVE-2015-5202**	https://bugzilla.redhat.com/show_bug.cgi?id=1253884	A-RED-SATEL-210617/158
Saat					
Netizen					
Gain Privileges	09-06-2017	6.8	Untrusted search path vulnerability in the installer of SaAT Netizen ver.1.2.10.510 and earlier allows an attacker to gain Gain Privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2206**	https://www.saat.jp/information/netizen/2017/0531_security_update_info.php	A-SAA-NETIZ-210617/159
Personal					
Gain Privileges	09-06-2017	6.8	Untrusted search path vulnerability in the installer of SaAT Personal ver.1.0.10.272 and	https://www.saat.jp/information/perso	A-SAA-PERSO-210617/

			earlier allows an attacker to gain Gain Privilegesileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2017-2207**	nal/2017/0531_security_update_info.php	160
Samba					
Samba					
DoS	06-06-2017	7.8	smbd in Samba before 4.4.10 and 4.5.x before 4.5.6 has a denial of service vulnerability (fd_open_atomic infinite loop with high CPU usage and memory consumption) due to wrongly handling dangling symlinks. **CVE ID: CVE-2017-9461**	https://bugs.debian.org/864291	A-SAM-SAMBA-210617/161
Samsung					
Syncthru 6					
Execute Code; Directory Traversal	01-06-2017	10	Multiple directory traversal vulnerabilities in Samsung SyncThru 6 before 1.0 allow remote attackers to delete arbitrary files via unspecified parameters to (1) upload/updateDriver or (2) upload/addDriver or to execute arbitrary code with SYSTEM Gain Privilegesileges via unspecified parameters to (3) uploadCloning.html, (4) fileupload.html, (5) uploadFirmware.html, or (6) upload/driver. **CVE ID: CVE-2015-5473**	NA	A-SAM-SYNCT-210617/162
Schneider-electric					
Somachine					
Overflow	07-06-2017	4.6	A buffer overflow vulnerability exists in Programming Software executable AlTracePrint.exe, in Schneider Electric's SoMachine HVAC v2.1.0 for Modicon M171/M172 Controller. **CVE ID: CVE-2017-7965**	http://www.schneider-electric.com/en/download/document/SEVD-2017-125-01/	A-SCH-SOMAC-210617/163
Execute Code	07-06-2017	6.8	A DLL Hijacking vulnerability in	http://www.s	A-SCH-

			the programming software in Schneider Electric's SoMachine HVAC v2.1.0 allows a remote attacker to execute arbitrary code on the targeted system. The vulnerability exists due to the improper loading of a DLL. **CVE ID: CVE-2017-7966**	chneider-electric.com/en/download/document/SEVD-2017-125-02/	SOMAC-210617/164
Simple Keitai Chat Project					
Simple Keitai Chat					
XSS	09-06-2017	4.3	Cross-site scripting vulnerability in Simple keitai chat 2.0 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE ID: CVE-2016-7817**	NA	A-SIM-SIMPL-210617/165
Skygroup					
Skysea Client View					
Execute Code	09-06-2017	10	SKYSEA Client View Ver.11.221.03 and earlier allows remote code execution via a flaw in processing authentication on the TCP connection with the management console program. **CVE ID: CVE-2016-7836**	https://www.skygroup.jp/security-info/170308.html	A-SKY-SKYSE-210617/166
Slideshow Project					
Slideshow					
info	08-06-2017	5	The SlideshowPluginSlideshowStylesheet::loadStylesheetByAJAX function in the Slideshow plugin 2.2.8 through 2.2.21 for Wordpress allows remote attackers to read arbitrary Wordpress option values. **CVE ID: CVE-2015-3634**	https://github.com/Boonstra/Slideshow/commit/cac505e593cbe70a4d8af5b639f5385d4cc7aa04	A-SLI-SLIDE-210617/167
Soffid					
IAM					
Execute Code	02-06-2017	7.5	Untrusted Java serialization in Soffid IAM console before 1.7.5 allows remote attackers to achieve arbitrary remote code execution via a crafted	http://www.soffid.com/security-advisory1-update/	A-SOF-IAM-210617/168

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

			authentication request. **CVE ID: CVE-2017-9363**		
Sophos					
Web Appliance					
XSS	08-06-2017	4.3	The Sophos Web Appliance before 4.3.2 has XSS in the FTP redirect page, aka NSWA-1342. **CVE ID: CVE-2017-9523**	http://swa.sophos.com/rn/swa/concepts/ReleaseNotes_4.3.2.html	A-SOP-WEB A-210617/169
Spiffy					
Spiffy					
Directory Traversal	07-06-2017	5	Directory traversal vulnerability in Spiffy before 5.4. **CVE ID: CVE-2015-8235**	http://code.call-cc.org/cgi-bin/gitweb.cgi?p=chicken-core.git;a=commit;h=edd4926bb4f4c97760a0e03b0d0e8210398fe967	A-SPI-SPIFF-210617/170
Subsonic					
Subsonic					
NA	07-06-2017	4.3	XML external entity (XXE) vulnerability in the import playlist feature in Subsonic 6.1.1 might allow remote attackers to conduct server-side request forgery (SSRF) attacks via a crafted XSPF playlist file. **CVE ID: CVE-2017-9355**	NA	A-SUB-SUBSO-210617/171
Sunnythemes					
Spiffy Calendar					
XSS	05-06-2017	4.3	Cross site scripting (XSS) vulnerability in the Spiffy Calendar plugin before 3.3.0 for WordPress allows remote attackers to inject arbitrary JavaScript via the yr parameter. **CVE ID: CVE-2017-9420**	NA	A-SUN-SPIFF-210617/172
Teampass					
Teampass					

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

Sql	05-06-2017	7.5	TeamPass before 2.1.27.4 is vulnerable to a SQL injection in users.queries.php. **CVE ID: CVE-2017-9436**	https://github.com/nilsteampassnet/TeamPass/blob/master/changelog.md	A-TEA-TEAMP-210617/173
Todd Miller					
Sudo					
Execute Code	05-06-2017	6.9	Todd Miller's sudo version 1.8.20 and earlier is vulnerable to an input validation (embedded spaces) in the get_process_ttyname() function resulting in information disclosure and command execution. **CVE ID: CVE-2017-1000367**	https://www.sudo.ws/alerts/linux_tty.html	A-TOD-SUDO-210617/174
Execute Code	05-06-2017	7.2	Todd Miller's sudo version 1.8.20p1 and earlier is vulnerable to an input validation (embedded newlines) in the get_process_ttyname() function resulting in information disclosure and command execution. **CVE ID: CVE-2017-1000368**	https://www.sudo.ws/alerts/linux_tty.html	A-TOD-SUDO-210617/175
Torproject					
Tor					
DoS	09-06-2017	5	The hidden-service feature in Tor before 0.3.0.8 allows a denial of service (assertion failure and daemon exit) in the connection_edge_process_relay_cell function via a BEGIN_DIR cell on a rendezvous circuit. **CVE ID: CVE-2017-0376**	https://github.com/torproject/tor/commit/56a7c5bc15e0447203a491c1ee37de9939ad1dcd	A-TOR-TOR-210617/176
DoS	09-06-2017	5	The hidden-service feature in Tor before 0.3.0.8 allows a denial of service (assertion failure and daemon exit) in the relay_send_end_cell_from_edge_ function via a malformed BEGIN cell.	https://github.com/torproject/tor/commit/79b59a2dfcb68897ee89d98587d09e55f07e68d7	A-TOR-TOR-210617/177

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

			CVE ID: CVE-2017-0375		
Unisys					
Mobigate					
Gain Information	09-06-2017	4.3	The mobiGate App for Android version 2.2.1.2 and earlier and mobiGate App for iOS version 2.2.4.1 and earlier do not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2016-7805**	NA	A-UNI-MOBIG-210617/178
Virustotal					
Yara					
DoS	05-06-2017	5	libyara/re.c in the regexp module in YARA 3.5.0 allows remote attackers to cause a denial of service (stack consumption) via a crafted rule (involving hex strings) that is mishandled in the _yr_re_emit function, a different vulnerability than CVE-2017-9304. **CVE ID: CVE-2017-9438**	https://github.com/VirusTotal/yara/issues/674	A-VIR-YARA-210617/179
DoS; Overflow; Gain Information	06-06-2017	5.8	The yr_arena_write_data function in YARA 3.6.1 allows remote attackers to cause a denial of service (buffer over-read and application crash) or obtain sensitive information from process memory via a crafted file that is mishandled in the yr_re_fast_exec function in libyara/re.c and the _yr_scan_match_callback function in libyara/scan.c. **CVE ID: CVE-2017-9465**	https://github.com/VirusTotal/yara/commit/992480c30f75943e9cd6245bb2015c7737f9b661	A-VIR-YARA-210617/180
Vmware					
Fusion;Workstation					
Execute Code; Overflow	08-06-2017	7.5	The drag-and-drop (DnD) function in VMware Workstation	https://www.vmware.com/	A-VMW-FUSIO-

			12.x before version 12.5.4 and Fusion 8.x before version 8.5.5 has an out-of-bounds memory access vulnerability. This may allow a guest to execute code on the operating system that runs Workstation or Fusion. **CVE ID: CVE-2017-4901**	security/advisories/VMSA-2017-0005.html	210617/181
Horizon View; Unified Access Gateway					
Execute Code; Overflow	08-06-2017	7.5	VMware Unified Access Gateway (2.5.x, 2.7.x, 2.8.x prior to 2.8.1) and Horizon View (7.x prior to 7.1.0, 6.x prior to 6.2.4) contain a heap buffer-overflow vulnerability which may allow a remote attacker to execute code on the security gateway. **CVE ID: CVE-2017-4907**	http://www.vmware.com/security/advisories/VMSA-2017-0008.html	A-VMW-HORIZ-210617/182
Horizon View; Workstation					
DoS; Execute Code; Overflow	08-06-2017	6.9	VMware Workstation (12.x prior to 12.5.3) and Horizon View Client (4.x prior to 4.4.0) contain an integer-overflow vulnerability in the True Type Font parser in the TPView.dll. On Workstation, this may allow a guest to execute code or perform a Denial of Service on the Windows OS that runs Workstation. In the case of a Horizon View Client, this may allow a View desktop to execute code or perform a Denial of Service on the Windows OS that runs the Horizon View Client. Exploitation is only possible if virtual printing has been enabled. This feature is not enabled by default on Workstation but it is enabled by default on Horizon View. **CVE ID: CVE-2017-4913**	http://www.vmware.com/security/advisories/VMSA-2017-0008.html	A-VMW-HORIZ-210617/183
DoS Execute Code	08-06-2017	6.9	VMware Workstation (12.x prior to 12.5.3) and Horizon View Client (4.x prior to 4.4.0) contain	http://www.vmware.com/security/advis	A-VMW-HORIZ-210617/

			multiple out-of-bounds read vulnerabilities in TrueType Font (TTF) parser in the TPView.dll. On Workstation, this may allow a guest to execute code or perform a Denial of Service on the Windows OS that runs Workstation. In the case of a Horizon View Client, this may allow a View desktop to execute code or perform a Denial of Service on the Windows OS that runs the Horizon View Client. Exploitation is only possible if virtual printing has been enabled. This feature is not enabled by default on Workstation but it is enabled by default on Horizon View. **CVE ID: CVE-2017-4912**	ories/VMSA-2017-0008.html	184
DoS Execute Code	08-06-2017	6.9	VMware Workstation (12.x prior to 12.5.3) and Horizon View Client (4.x prior to 4.4.0) contain multiple out-of-bounds write vulnerabilities in JPEG2000 parser in the TPView.dll. On Workstation, this may allow a guest to execute code or perform a Denial of Service on the Windows OS that runs Workstation. In the case of a Horizon View Client, this may allow a View desktop to execute code or perform a Denial of Service on the Windows OS that runs the Horizon View Client. Exploitation is only possible if virtual printing has been enabled. This feature is not enabled by default on Workstation but it is enabled by default on Horizon View. **CVE ID: CVE-2017-4911**	http://www.vmware.com/security/advisories/VMSA-2017-0008.html	A-VMW-HORIZ-210617/185
DoS Execute	08-06-2017	6.9	VMware Workstation (12.x prior	http://www.v	A-VMW-

Code			to 12.5.3) and Horizon View Client (4.x prior to 4.4.0) contain multiple out-of-bounds read vulnerabilities in JPEG2000 parser in the TPView.dll. On Workstation, this may allow a guest to execute code or perform a Denial of Service on the Windows OS that runs Workstation. In the case of a Horizon View Client, this may allow a View desktop to execute code or perform a Denial of Service on the Windows OS that runs the Horizon View Client. Exploitation is only possible if virtual printing has been enabled. This feature is not enabled by default on Workstation but it is enabled by default on Horizon View. **CVE ID: CVE-2017-4910**	mware.com/security/advisories/VMSA-2017-0008.html	HORIZ-210617/186
DoS Execute Code Overflow	08-06-2017	6.9	VMware Workstation (12.x prior to 12.5.3) and Horizon View Client (4.x prior to 4.4.0) contain a heap buffer-overflow vulnerability in TrueType Font (TTF) parser in the TPView.dll. On Workstation, this may allow a guest to execute code or perform a Denial of Service on the Windows OS that runs Workstation. In the case of a Horizon View Client, this may allow a View desktop to execute code or perform a Denial of Service on the Windows OS that runs the Horizon View Client. Exploitation is only possible if virtual printing has been enabled. This feature is not enabled by default on Workstation but it is enabled by default on Horizon View.	http://www.vmware.com/security/advisories/VMSA-2017-0008.html	A-VMW-HORIZ-210617/187

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

			CVE ID: CVE-2017-4909		
DoS Execute Code Overflow	08-06-2017	6.9	VMware Workstation (12.x prior to 12.5.3) and Horizon View Client (4.x prior to 4.4.0) contain multiple heap buffer-overflow vulnerabilities in JPEG2000 parser in the TPView.dll. On Workstation, this may allow a guest to execute code or perform a Denial of Service on the Windows OS that runs Workstation. In the case of a Horizon View Client, this may allow a View desktop to execute code or perform a Denial of Service on the Windows OS that runs the Horizon View Client. Exploitation is only possible if virtual printing has been enabled. This feature is not enabled by default on Workstation but it is enabled by default on Horizon View. **CVE ID: CVE-2017-4908**	http://www.vmware.com/security/advisories/VMSA-2017-0008.html	A-VMW-HORIZ-210617/188
Vsphere Data Protection					
Gain Information	07-06-2017	5	VMware vSphere Data Protection (VDP) 6.1.x, 6.0.x, 5.8.x, and 5.5.x locally stores vCenter Server credentials using reversible encryption. This issue may allow plaintext credentials to be obtained. **CVE ID: CVE-2017-4917**	http://www.vmware.com/security/advisories/VMSA-2017-0010.html	A-VMW-VSPHE-210617/189
Execute Code	07-06-2017	7.5	VMware vSphere Data Protection (VDP) 6.1.x, 6.0.x, 5.8.x, and 5.5.x contains a deserialization issue. Exploitation of this issue may allow a remote attacker to execute commands on the appliance. **CVE ID: CVE-2017-4914**	http://www.vmware.com/security/advisories/VMSA-2017-0010.html	A-VMW-VSPHE-210617/190
Workstation Player; Workstation Pro					
NA	07-06-2017	6.9	VMware Workstation Pro/Player 12.x before 12.5.3 contains a DLL	http://www.vmware.com/s	A-VMW-WORKS-

			loading vulnerability that occurs due to the "vmware-vmx" process loading DLLs from a path defined in the local environment-variable. Successful exploitation of this issue may allow normal users to escalate Gain Privileges to System in the host machine where VMware Workstation is installed. **CVE ID: CVE-2017-4898**	ecurity/advisories/VMSA-2017-0003.html	210617/191
Websitebaker					
Websitebaker					
XSS	02-06-2017	4.3	WebsiteBaker v2.10.0 has a stored XSS vulnerability in /account/details.php. **CVE ID: CVE-2017-9361**	https://jgj212.blogspot.tw/2017/05/a-stored-xss-vulnerability-in.html	A-WEB-WEBSI-210617/192
Sql	02-06-2017	7.5	WebsiteBaker v2.10.0 has SQL injection vulnerability in /account/details.php. **CVE ID: CVE-2017-9360**	https://jgj212.blogspot.tw/2017/05/a-sql-injection-vulnerability-in.html	A-WEB-WEBSI-210617/193
Winsparkle					
Winsparkle					
Execute Code	09-06-2017	6.8	Untrusted search path vulnerability in WinSparkle versions prior to 0.5.3 allows remote attackers to execute arbitrary code via a specially crafted executable file in an unspecified directory. **CVE ID: CVE-2016-7838**	https://www.wireshark.org/news/20161214.html	A-WIN-WINSP-210617/194
Wireshark					
Wireshark					
NA	14-06-2017	4.3	In Wireshark 2.2.7, overly deep mp4 chunks may cause stack exhaustion (uncontrolled recursion) in the dissect_mp4_box function in epan/dissectors/file-mp4.c. **CVE ID: CVE-2017-9616**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=13777	A-WIR-WIRES-210617/195

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	02-06-2017	5	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the RGMP dissector could crash. This was addressed in epan/dissectors/packet-rgmp.c by validating an IPv4 address. **CVE ID: CVE-2017-9354**	NA	A-WIR-WIRES-210617/196
NA	02-06-2017	5	In Wireshark 2.2.0 to 2.2.6, the IPv6 dissector could crash. This was addressed in epan/dissectors/packet-ipv6.c by validating an IPv6 address. **CVE ID: CVE-2017-9353**	NA	A-WIR-WIRES-210617/197
Overflow	02-06-2017	5	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the DHCP dissector could read past the end of a buffer. This was addressed in epan/dissectors/packet-bootp.c by extracting the Vendor Class Identifier more carefully. **CVE ID: CVE-2017-9351**	NA	A-WIR-WIRES-210617/198
Overflow	02-06-2017	5	In Wireshark 2.2.0 to 2.2.6, the DOF dissector could read past the end of a buffer. This was addressed in epan/dissectors/packet-dof.c by validating a size value. **CVE ID: CVE-2017-9348**	NA	A-WIR-WIRES-210617/199
NA	02-06-2017	5	In Wireshark 2.2.0 to 2.2.6, the ROS dissector could crash with a NULL pointer dereference. This was addressed in epan/dissectors/asn1/ros/packet-ros-template.c by validating an OID. **CVE ID: CVE-2017-9347**	NA	A-WIR-WIRES-210617/200
NA	02-06-2017	5	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the Bluetooth L2CAP dissector could divide by zero. This was addressed in epan/dissectors/packet-btl2cap.c by validating an interval value. **CVE ID: CVE-2017-9344**	NA	A-WIR-WIRES-210617/201
NA	02-06-2017	5	In Wireshark 2.2.0 to 2.2.6 and	NA	A-WIR-

			2.0.0 to 2.0.12, the MSNIP dissector misuses a NULL pointer. This was addressed in epan/dissectors/packet-msnip.c by validating an IPv4 address. **CVE ID: CVE-2017-9343**		WIRES-210617/202
NA	14-06-2017	5	In Wireshark 2.2.7, deeply nested DAAP data may cause stack exhaustion (uncontrolled recursion) in the dissect_daap_one_tag function in epan/dissectors/packet-daap.c in the DAAP dissector. **CVE ID: CVE-2017-9617**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=13799	A-WIR-WIRES-210617/203
NA	02-06-2017	7.8	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the Bazaar dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-bzr.c by ensuring that backwards parsing cannot occur. **CVE ID: CVE-2017-9352**	NA	A-WIR-WIRES-210617/204
NA	02-06-2017	7.8	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the openSAFETY dissector could crash or exhaust system memory. This was addressed in epan/dissectors/packet-opensafety.c by checking for a negative length. **CVE ID: CVE-2017-9350**	NA	A-WIR-WIRES-210617/205
NA	02-06-2017	7.8	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the DICOM dissector has an infinite loop. This was addressed in epan/dissectors/packet-dcm.c by validating a length value. **CVE ID: CVE-2017-9349**	NA	A-WIR-WIRES-210617/206
NA	02-06-2017	7.8	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the SoulSeek dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-slsk.c by making loop bounds more	NA	A-WIR-WIRES-210617/207

			explicit. **CVE ID: CVE-2017-9346**		
NA	02-06-2017	7.8	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the DNS dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-dns.c by trying to detect self-referencing pointers. **CVE ID: CVE-2017-9345**	NA	A-WIR-WIRES-210617/208
Wordpress Backup To Dropbox Project					
Wordpress Backup To Dropbox					
XSS	07-06-2017	4.3	Cross-site scripting (XSS) vulnerability in the WordPress Backup to Dropbox plugin before 4.1 for WordPress. **CVE ID: CVE-2014-9310**	https://wordpress.org/plugins/wordpress-backup-to-dropbox/	A-WOR-WORDP-210617/209
Wp Editor.md Project					
Wp Editor.md					
XSS	01-06-2017	4.3	The WP Editor.MD plugin 1.6 for WordPress has a stored XSS vulnerability in the content of a post. **CVE ID: CVE-2017-9336**	http://lncken.cn/?p=258	A-WP - WP ED-210617/210
Ytnef Project					
Ytnef					
DoS Overflow	07-06-2017	4.3	In ytnef 1.9.2, the DecompressRTF function in lib/ytnef.c allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file. **CVE ID: CVE-2017-9474**	https://blogs.gentoo.org/ago/2017/05/24/ytnef-heap-based-buffer-overflow-in-decompressrtf-ytnef-c/	A-YTN-YTNEF-210617/211
DoS	07-06-2017	4.3	In ytnef 1.9.2, the TNEFFillMapi function in lib/ytnef.c allows remote attackers to cause a denial of service (memory consumption) via a crafted file. **CVE ID: CVE-2017-9473**	https://blogs.gentoo.org/ago/2017/05/24/ytnef-memory-allocation-failure-in-tneffillmapi-ytnef-c/	A-YTN-YTNEF-210617/212

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 Overflow	07-06-2017	4.3	In ytnef 1.9.2, the SwapDWord function in lib/ytnef.c allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file. **CVE ID: CVE-2017-9472**	https://blogs.gentoo.org/ago/2017/05/24/ytnef-heap-based-buffer-overflow-in-swapdword-ytnef-c/	A-YTN-YTNEF-210617/213
DoS Overflow	07-06-2017	4.3	In ytnef 1.9.2, the SwapWord function in lib/ytnef.c allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file. **CVE ID: CVE-2017-9471**	https://blogs.gentoo.org/ago/2017/05/24/ytnef-heap-based-buffer-overflow-in-swapword-ytnef-c/	A-YTN-YTNEF-210617/214
DoS	07-06-2017	4.3	In ytnef 1.9.2, the MAPIPrint function in lib/ytnef.c allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file. **CVE ID: CVE-2017-9470**	https://blogs.gentoo.org/ago/2017/05/24/ytnef-null-pointer-dereference-in-mapiprint-ytnef-c/	A-YTN-YTNEF-210617/215
Zcms					
Sql	07-06-2017	7.5	SQL injection vulnerability in ZCMS 1.1. **CVE ID: CVE-2015-7346**	NA	A-ZCM-ZCMS-210617/216
Zend					
Zend Framework					
CSRF	08-06-2017	6.8	Cross-site request forgery (CSRF) vulnerability in Zend/Validator/Csrf in Zend Framework 2.3.x before 2.3.6 via null or malformed token identifiers. **CVE ID: CVE-2015-1786**	https://bugzilla.redhat.com/show_bug.cgi?id=1207781	A-ZEN-ZEND - 210617/217
Application/ Operating System (A/OS)					
Canonical;Debian;Fedoraproject;Novell/GIT					
Ubuntu Linux/Debian Linux/Fedora/Leap/Git-shell					
Gain Privileges	01-06-2017	6.5	git-shell in git before 2.4.12, 2.5.x before 2.5.6, 2.6.x before 2.6.7,	https://kernel.googlesource.	A-OS-CAN-

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

			2.7.x before 2.7.5, 2.8.x before 2.8.5, 2.9.x before 2.9.4, 2.10.x before 2.10.3, 2.11.x before 2.11.2, and 2.12.x before 2.12.3 might allow remote authenticated users to gain Gain Privileges via a repository name that starts with a - (dash) character. **CVE ID: CVE-2017-8386**	com/pub/scm/git/git/+/3ec804490a265f4c418a321428c12f3f18b7eff5	UBUNT-210617/218
Fedoraproject;Novell;Opensuse Project/Game-music-emu Project					
Fedora/Suse Linux Enterprise Desktop;Suse Linux Enterprise Server;Suse Linux Enterprise Software Development Kit/Leap/Game-music-emu					
NA	06-06-2017	10	game-music-emu before 0.6.1 mishandles unspecified integer values. **CVE ID: CVE-2016-9961**	https://bugzilla.redhat.com/show_bug.cgi?id=1405423	A-OS-FED-FEDOR-210617/219
PHP/Suse					
PHP/Linux Enterprise Module For Web Scripting;Linux Enterprise Software Development Kit					
Execute Code	08-06-2017	7.5	/ext/phar/phar_object.c in PHP 7.0.7 and 5.6.x allows remote attackers to execute arbitrary code. NOTE: Introduced as part of an incomplete fix to CVE-2015-6833. **CVE ID: CVE-2016-4473**	https://bugzilla.redhat.com/show_bug.cgi?id=1347772	A-OS-PHP-PHP/L-210617/220
Vmware/Vmware					
Esxi/Fusion;Fusion Pro;Workstation Player;Workstation Pro					
Execute Code; Overflow	07-06-2017	7.2	VMware ESXi 6.5 without patch ESXi650-201703410-SG and 5.5 without patch ESXi550-201703401-SG; Workstation Pro / Player 12.x prior to 12.5.5; and Fusion Pro / Fusion 8.x prior to 8.5.6 have a Heap Buffer Overflow in SVGA. This issue may allow a guest to execute code on the host. **CVE ID: CVE-2017-4902**	http://www.vmware.com/security/advisories/VMSA-2017-0006.html	A-OS-VMW-ESXI/-210617/221
Esxi/Fusion;Workstation Player;Workstation Pro					
DoS; Execute Code; Overflow	07-06-2017	7.2	The XHCI controller in VMware ESXi 6.5 without patch ESXi650-201703410-SG, 6.0 U3 without	http://www.vmware.com/security/advis	A-OS-VMW-ESXI/-

			patch ESXi600-201703401-SG, 6.0 U2 without patch ESXi600-201703403-SG, 6.0 U1 without patch ESXi600-201703402-SG, and 5.5 without patch ESXi550-201703401-SG; Workstation Pro / Player 12.x prior to 12.5.5; and Fusion Pro / Fusion 8.x prior to 8.5.6 has uninitialized memory usage. This issue may allow a guest to execute code on the host. The issue is reduced to a Denial of Service of the guest on ESXi 5.5. **CVE ID: CVE-2017-4904**	ories/VMSA-2017-0006.html	210617/222
Execute Code Overflow	07-06-2017	7.2	VMware ESXi 6.5 without patch ESXi650-201703410-SG, 6.0 U3 without patch ESXi600-201703401-SG, 6.0 U2 without patch ESXi600-201703403-SG, 6.0 U1 without patch ESXi600-201703402-SG, and 5.5 without patch ESXi550-201703401-SG; Workstation Pro / Player 12.x prior to 12.5.5; and Fusion Pro / Fusion 8.x prior to 8.5.6 have an uninitialized stack memory usage in SVGA. This issue may allow a guest to execute code on the host. **CVE ID: CVE-2017-4903**	http://www.vmware.com/security/advisories/VMSA-2017-0006.html	A-OS-VMW-ESXI/-210617/223
Operating System (OS)					
Broadcom					
Bcm43xx Wi-fi Chipset Firmware					
Execute Code	04-06-2017	7.5	Broadcom BCM43xx Wi-Fi chips allow remote attackers to execute arbitrary code via unspecified vectors, aka the "Broadpwn" issue. **CVE ID: CVE-2017-9417**	https://www.blackhat.com/us-17/briefings.html#broadpwn-remotely-compromising-android-and-ios-via-a-bug-in-	O-BRO-BCM43-210617/224

				broadcoms-wi-fi-chipsets	
Buffalotech					
Wnc01wh Firmware					
DoS	09-06-2017	4.3	Buffalo WNC01WH devices with firmware version 1.0.0.8 and earlier allow remote attackers to cause a denial of service against the management screen via unspecified vectors. **CVE ID: CVE-2016-7821**	http://buffalo.jp/support_s/s20161201.html	O-BUF-WNC01-210617/225
Bypass	09-06-2017	6.5	Buffalo NC01WH devices with firmware version 1.0.0.8 and earlier allows authenticated attackers to bypass access restriction to enable the debug option via unspecified vectors. **CVE ID: CVE-2016-7824**	http://buffalo.jp/support_s/s20161201.html	O-BUF-WNC01-210617/226
CSRF	09-06-2017	6.8	Cross-site request forgery (CSRF) vulnerability in Buffalo WNC01WH devices with firmware version 1.0.0.8 and earlier allows remote attackers to hijack the authentication of a logged in user to perform unintended operations via unspecified vectors. **CVE ID: CVE-2016-7822**	http://buffalo.jp/support_s/s20161201.html	O-BUF-WNC01-210617/227
Ceragon					
Fiberair Ip-10 Firmware					
NA	01-06-2017	7.5	Ceragon FibeAir IP-10 have a default SSH public key in the authorized_keys file for the mateidu user, which allows remote attackers to obtain SSH access by leveraging knowledge of the Gain Privileges key. **CVE ID: CVE-2015-0936**	NA	O-CER-FIBER-210617/228
Compulab					
Intense Pc Firmware; Mintbox 2 Firmware					
NA	06-06-2017	7.2	CompuLab Intense PC and MintBox 2 devices with BIOS before 2017-05-21 do not use the CloseMnf	NA	O-COM-INTEN-210617/

			protection mechanism for write protection of flash memory regions, which allows local users to install a firmware rootkit by leveraging administrative Gain Privilegesileges. **CVE ID: CVE-2017-8083**		229
Corega					
Cg-wlbaragm Firmware; Cg-wlbargnl Firmware					
XSS	09-06-2017	4.3	Cross-site scripting vulnerability in Corega CG-WLBARGMH and CG-WLBARGNL allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE ID: CVE-2016-7808**	http://corega.jp/support/security/20161111_wlbargmh_wlbargnl.htm	O-COR-CG-WL-210617/230
Cg-wlr300nx Firmware					
Bypass	09-06-2017	5.8	Corega CG-WLR300NX firmware Ver. 1.20 and earlier allows an attacker on the same network segment to bypass access restriction to perform arbitrary operations via unspecified vectors. **CVE ID: CVE-2016-7811**	http://corega.jp/support/security/20161111_wlr300nx.htm	O-COR-CG-WL-210617/231
CSRF	09-06-2017	6.8	Cross-site request forgery (CSRF) vulnerability in Corega CG-WLR300NX firmware Ver. 1.20 and earlier allows remote attackers to hijack the authentication of logged in user to conduct unintended operations via unspecified vectors. **CVE ID: CVE-2016-7809**	http://corega.jp/support/security/20161111_wlr300nx.htm	O-COR-CG-WL-210617/232
Fortinet					
Fortios					
Execute Code XSS	01-06-2017	4.3	A Cross-Site Scripting vulnerability in Fortinet FortiGate 5.2.0 through 5.2.10 allows attacker to execute unauthorized code or commands via the srcintf parameter during Firewall Policy Creation. **CVE ID: CVE-2017-3127**	https://fortiguard.com/psirt/FG-IR-17-017	O-FOR-FORTI-210617/233

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

Google					
Android					
NA	06-06-2017	4.3	The stock Android browser address bar in all Android operating systems suffers from Address Bar Spoofing, which allows remote attackers to trick a victim by displaying a malicious page for legitimate domain names. **CVE ID: CVE-2015-3830**	NA	O-GOO-ANDRO-210617/234
Gain Information	06-06-2017	4.3	In TrustZone in all Android releases from CAF using the Linux kernel, an Information Exposure Through Timing Discrepancy vulnerability could potentially exist. **CVE ID: CVE-2014-9951**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/235
Gain Information	06-06-2017	4.3	In TrustZone in all Android releases from CAF using the Linux kernel, an Information Exposure vulnerability could potentially exist. **CVE ID: CVE-2014-9947**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/236
NA	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, a race condition exists in a QTEE driver potentially leading to an arbitrary memory write. **CVE ID: CVE-2017-8242**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/237
Gain Information	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, userspace-controlled parameters for flash initialization are not sanitized potentially leading to exposure of kernel memory. **CVE ID: CVE-2017-8239**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/238
NA	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, a memory structure in a camera driver is not properly protected. **CVE ID: CVE-2017-8235**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/239
NA	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, a KGSL ioctl was not validating all of its	https://source.android.com/security	O-GOO-ANDRO-210617/

			parameters. **CVE ID: CVE-2017-7366**	/bulletin/2017-06-01	240
NA	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, some validation of secure applications was not being performed. **CVE ID: CVE-2016-10337**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/241
NA	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, some regions of memory were not protected during boot. **CVE ID: CVE-2016-10336**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/242
NA	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, libtomcrypt was updated. **CVE ID: CVE-2016-10335**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/243
NA	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, a dynamically-protected DDR region could potentially get overwritten. **CVE ID: CVE-2016-10334**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/244
NA	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, a sensitive system call was allowed to be called by HLOS. **CVE ID: CVE-2016-10333**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/245
NA	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, stack protection was not enabled for secure applications. **CVE ID: CVE-2016-10332**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/246
Gain Information	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, a DRM key was exposed to QTEE applications. **CVE ID: CVE-2015-9032**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/247
Gain Information	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, a TZ memory address is exposed to HLOS by HDCP. **CVE ID: CVE-2015-9031**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/248
NA	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, some	https://source.android.c	O-GOO-ANDRO-

			interfaces were improperly exposed to QTEE applications. **CVE ID: CVE-2015-9024**	om/security /bulletin/2017-06-01	210617/249
NA	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, access control to SMEM memory was not enabled. **CVE ID: CVE-2015-9021**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/250
info	14-06-2017	4.3	An information disclosure vulnerability in libziparchive could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access sensitive data without permission. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-36392138. **CVE ID: CVE-2017-0647**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/251
info	14-06-2017	4.3	An information disclosure vulnerability in Bluetooth component could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate due to details specific to the vulnerability. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-33899337. **CVE ID: CVE-2017-0646**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/252
Bypass Gain Information	14-06-2017	4.3	An elevation of Gain Privileges vulnerability in Bluetooth could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it is a local bypass of user interaction requirements. Product: Android. Versions: 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-35385327. **CVE ID: CVE-2017-0645**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/253
Bypass Gain	14-06-2017	4.3	Information disclosure	https://sour	O-GOO-

Information			vulnerability in Bluetooth component could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it is a general bypass for operating system protections that isolate application data from other applications. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-35310991. **CVE ID: CVE-2017-0639**	ce.android.com/security/bulletin/2017-06-01	ANDRO-210617/254
DoS	08-06-2017	5	b/libs/gui/ISurfaceComposer.cpp in Android allows attackers to trigger a denial of service (null pointer dereference and process crash). **CVE ID: CVE-2014-7919**	https://github.com/alexpark07/Bookmark/issues/1	O-GOO-ANDRO-210617/255
Gain Information	13-06-2017	5.8	In all Android releases from CAF using the Linux kernel, HLOS can overwite secure memory or read contents of the keystore. **CVE ID: CVE-2016-10339**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/256
Execute Code	14-06-2017	6.8	A remote code execution vulnerability in libxml2 could enable an attacker using a specially crafted file to execute arbitrary code within the context of an unGain Privilegesileged process. This issue is rated as High due to the possibility of remote code execution in an application that uses this library. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37104170. **CVE ID: CVE-2017-0663**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/257
Execute Code	14-06-2017	6.8	A remote code execution vulnerability in System UI component could enable an attacker using a specially crafted file to execute arbitrary code within the context of an unGain	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/258

			Privilegesileged process. This issue is rated as High because it is a remote arbitrary code execution in an unGain Privilegesileged process. Product: Android. Versions: 7.1.1, 7.1.2. Android ID: A-36368305. **CVE ID: CVE-2017-0638**		
DoS	14-06-2017	7.1	A remote denial of service vulnerability in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1. Android ID: A-35472997. **CVE ID: CVE-2017-0644**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/259
DoS	14-06-2017	7.1	A remote denial of service vulnerability in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-35645051. **CVE ID: CVE-2017-0643**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/260
DoS	14-06-2017	7.1	A remote denial of service vulnerability in libhevc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-34819017. **CVE ID: CVE-2017-0642**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/261
DoS	14-06-2017	7.1	A remote denial of service vulnerability in libvpx in	https://source.android.c	O-GOO-ANDRO-

			Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-34360591. **CVE ID: CVE-2017-0641**	om/security/bulletin/2017-06-01	210617/262
DoS	14-06-2017	7.1	A remote denial of service vulnerability in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33129467. **CVE ID: CVE-2017-0640**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/263
NA	06-06-2017	7.6	In the Embedded File System in all Android releases from CAF using the Linux kernel, a Time-of-Check Time-of-Use Race Condition vulnerability could potentially exist. **CVE ID: CVE-2014-9941**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/264
Overflow	13-06-2017	7.6	In all Android releases from CAF using the Linux kernel, a race condition exists in a video driver potentially leading to buffer overflow or write to arbitrary pointer location. **CVE ID: CVE-2017-7372**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/265
NA	13-06-2017	7.6	In all Android releases from CAF using the Linux kernel, a race condition exists in a video driver potentially leading to a use-after-free condition. **CVE ID: CVE-2017-7370**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/266
NA	13-06-2017	7.6	In all Android releases from CAF using the Linux kernel, a race condition potentially exists in the	https://source.android.com/security	O-GOO-ANDRO-210617/

			ioctl handler of a sound driver. **CVE ID: CVE-2017-7368**	/bulletin/2017-06-01	267
NA	13-06-2017	7.6	In all Android releases from CAF using the Linux kernel, time-of-check Time-of-use (TOCTOU) Race Conditions exist in several TZ APIs. **CVE ID: CVE-2015-9022**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/268
NA	13-06-2017	7.6	In all Android releases from CAF using the Linux kernel, a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability exists in Secure Display. **CVE ID: CVE-2014-9966**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/269
Execute Code	14-06-2017	7.6	An elevation of Gain Privilegesilege vulnerability in the MediaTek sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Moderate because it first requires compromising a Gain Privilegesileged process and because of vulnerability specific details which limit the impact of the issue. Product: Android. Versions: N/A. Android ID: A-34468195. References: M-ALPS03162283. **CVE ID: CVE-2017-0649**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/270
NA	06-06-2017	9.3	In TrustZone in all Android releases from CAF using the Linux kernel, a Time-of-Check Time-of-Use Race Condition vulnerability could potentially exist. **CVE ID: CVE-2016-10297**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/271
NA	06-06-2017	9.3	In TrustZone in all Android releases from CAF using the Linux kernel, a Double Free vulnerability could potentially exist. **CVE ID: CVE-2015-9007**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/272
NA	06-06-2017	9.3	In Resource Power Manager (RPM) in all Android releases from CAF using the Linux kernel, an Improper Access Control	https://source.android.com/security/bulletin/20	O-GOO-ANDRO-210617/273

			vulnerability could potentially exist. **CVE ID: CVE-2015-9006**	17-05-01	
Overflow	06-06-2017	9.3	In TrustZone in all Android releases from CAF using the Linux kernel, an Integer Overflow to Buffer Overflow vulnerability could potentially exist. **CVE ID: CVE-2015-9005**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/274
NA	06-06-2017	9.3	In the Secure File System in all Android releases from CAF using the Linux kernel, a capture-replay vulnerability could potentially exist. **CVE ID: CVE-2014-9952**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/275
NA	06-06-2017	9.3	In Core Kernel in all Android releases from CAF using the Linux kernel, an Improper Authorization vulnerability could potentially exist. **CVE ID: CVE-2014-9950**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/276
NA	06-06-2017	9.3	In TrustZone in all Android releases from CAF using the Linux kernel, an Untrusted Pointer Dereference vulnerability could potentially exist. **CVE ID: CVE-2014-9949**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/277
NA	06-06-2017	9.3	In TrustZone in all Android releases from CAF using the Linux kernel, an Improper Validation of Array Index vulnerability could potentially exist. **CVE ID: CVE-2014-9948**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/278
NA	06-06-2017	9.3	In Core Kernel in all Android releases from CAF using the Linux kernel, a Use After Free vulnerability could potentially exist. **CVE ID: CVE-2014-9946**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/279
NA	06-06-2017	9.3	In TrustZone in all Android releases from CAF using the Linux kernel, an Improper Authorization vulnerability could potentially exist.	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/280

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

			CVE ID: CVE-2014-9945		
Overflow	06-06-2017	9.3	In the Secure File System in all Android releases from CAF using the Linux kernel, an Integer Overflow to Buffer Overflow vulnerability could potentially exist. **CVE ID: CVE-2014-9944**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/281
NA	06-06-2017	9.3	In Core Kernel in all Android releases from CAF using the Linux kernel, a Null Pointer Dereference vulnerability could potentially exist. **CVE ID: CVE-2014-9943**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/282
NA	06-06-2017	9.3	In Boot in all Android releases from CAF using the Linux kernel, a Use of Uninitialized Variable vulnerability could potentially exist. **CVE ID: CVE-2014-9942**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/283
NA	06-06-2017	9.3	In WCDMA in all Android releases from CAF using the Linux kernel, a Use After Free vulnerability could potentially exist. **CVE ID: CVE-2014-9930**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/284
Overflow	06-06-2017	9.3	In WCDMA in all Android releases from CAF using the Linux kernel, a Use of Out-of-range Pointer Offset vulnerability could potentially exist. **CVE ID: CVE-2014-9929**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/285
Overflow	06-06-2017	9.3	In GERAN in all Android releases from CAF using the Linux kernel, a Buffer Copy without Checking Size of Input vulnerability could potentially exist. **CVE ID: CVE-2014-9928**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/286
Overflow	06-06-2017	9.3	In UIM in all Android releases from CAF using the Linux kernel, a Buffer Copy without Checking Size of Input vulnerability could potentially exist. **CVE ID: CVE-2014-9927**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/287
NA	06-06-2017	9.3	In GNSS in all Android releases	https://sour	O-GOO-

			from CAF using the Linux kernel, a Use After Free vulnerability could potentially exist. **CVE ID: CVE-2014-9926**	ce.android.com/security/bulletin/2017-05-01	ANDRO-210617/288
Overflow	06-06-2017	9.3	In HDR in all Android releases from CAF using the Linux kernel, a Buffer Copy without Checking Size of Input vulnerability could potentially exist. **CVE ID: CVE-2014-9925**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/289
NA	06-06-2017	9.3	In 1x in all Android releases from CAF using the Linux kernel, a Signed to Unsigned Conversion Error could potentially occur. **CVE ID: CVE-2014-9924**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/290
Overflow	06-06-2017	9.3	In NAS in all Android releases from CAF using the Linux kernel, a Buffer Copy without Checking Size of Input vulnerability could potentially exist. **CVE ID: CVE-2014-9923**	https://source.android.com/security/bulletin/2017-05-01	O-GOO-ANDRO-210617/291
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in a WLAN function due to an incorrect message length. **CVE ID: CVE-2017-8241**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/292
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a kernel driver has an off-by-one buffer over-read vulnerability. **CVE ID: CVE-2017-8240**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/293
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in a camera function. **CVE ID: CVE-2017-8238**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/294
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists while loading a firmware image. **CVE ID: CVE-2017-8237**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/295
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a buffer	https://source.android.c	O-GOO-ANDRO-

			overflow vulnerability exists in an IPA driver. **CVE ID: CVE-2017-8236**	om/security/bulletin/2017-06-01	210617/296
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, an out of bounds access can potentially occur in a camera function. **CVE ID: CVE-2017-8234**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/297
NA	13-06-2017	9.3	In a camera driver function in all Android releases from CAF using the Linux kernel, a bounds check is missing when writing into an array potentially leading to an out-of-bounds heap write. **CVE ID: CVE-2017-8233**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/298
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a double free vulnerability exists in a display driver. **CVE ID: CVE-2017-7373**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/299
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a data pointer is potentially used after it has been freed when SLIMbus is turned off by Bluetooth. **CVE ID: CVE-2017-7371**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/300
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, an array index in an ALSA routine is not properly validating potentially leading to kernel stack corruption. **CVE ID: CVE-2017-7369**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/301
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, an integer underflow vulnerability exists while processing the boot image. **CVE ID: CVE-2017-7367**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/302
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a buffer overread can occur if a particular string is not NULL terminated. **CVE ID: CVE-2017-7365**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/303
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a buffer	https://source.android.c	O-GOO-ANDRO-

			overflow vulnerability exists in a syscall handler. **CVE ID: CVE-2016-10342**	om/security/bulletin/2017-06-01	210617/304
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, 3rd party TEEs have more Gain Privilegesilege than intended. **CVE ID: CVE-2016-10341**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/305
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, an integer underflow leading to buffer overflow vulnerability exists in a syscall handler. **CVE ID: CVE-2016-10340**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/306
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, there was an issue related to RPMB processing. **CVE ID: CVE-2016-10338**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/307
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a QTEE system call fails to validate a pointer. **CVE ID: CVE-2015-9033**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/308
Bypass	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, the Hypervisor API could be misused to bypass authentication. **CVE ID: CVE-2015-9030**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/309
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a vulnerability exists in the access control settings of modem memory. **CVE ID: CVE-2015-9029**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/310
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in a cryptographic routine. **CVE ID: CVE-2015-9028**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/311
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, an untrusted pointer dereference vulnerability exists in WideVine	https://source.android.com/security/bulletin/20	O-GOO-ANDRO-210617/312

			DRM. **CVE ID: CVE-2015-9027**	17-06-01	
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, an untrusted pointer dereference vulnerability exists in WideVine DRM. **CVE ID: CVE-2015-9026**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/313
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in a QTEE application. **CVE ID: CVE-2015-9025**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/314
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in the PlayReady API. **CVE ID: CVE-2015-9023**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/315
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, an untrusted pointer dereference vulnerability exists in the unlocking of memory. **CVE ID: CVE-2015-9020**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/316
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, an untrusted pointer dereference vulnerability exists in WideVine DRM. **CVE ID: CVE-2014-9967**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/317
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a vulnerability exists in the parsing of an SCM call. **CVE ID: CVE-2014-9965**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/318
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, an integer overflow vulnerability exists in debug functionality. **CVE ID: CVE-2014-9964**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/319
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in WideVine DRM.	https://source.android.com/security/bulletin/20	O-GOO-ANDRO-210617/320

			CVE ID: CVE-2014-9963	17-06-01	
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a vulnerability exists in the parsing of a DRM provisioning command. **CVE ID: CVE-2014-9962**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/321
Bypass	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a vulnerability in eMMC write protection exists that can be used to bypass power-on write protection. **CVE ID: CVE-2014-9961**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/322
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in the PlayReady API. **CVE ID: CVE-2014-9960**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/323
Execute Code Overflow Memory Corruption	14-06-2017	9.3	A remote code execution vulnerability in libhevc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process.Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-34064500. **CVE ID: CVE-2017-0637**	https://source.android.com/security/bulletin/2017-06-01	O-GOO-ANDRO-210617/324
Huawei					
Ar1220 Firmware					
DoS	08-06-2017	4.3	Huawei AR1220 routers with software before V200R005SPH006 allow remote attackers to cause a denial of service (board reset) via vectors involving a large amount of traffic from the GE port to the FE port. **CVE ID: CVE-2015-2255**	http://www.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-	O-HUA-AR122-210617/325

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

				417840.htm	
Oceanstor Uds Firmware					
Gain Information	08-06-2017	5	The DeviceManager in Huawei OceanStor UDS devices with software before V100R002C01SPC102 might allow remote attackers to obtain sensitive information via a crafted UDS patch with JavaScript. **CVE ID: CVE-2015-2251**	http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-417837.htm	O-HUA-OCEAN-210617/326
Execute Code	08-06-2017	9.3	Huawei OceanStor UDS devices with software before V100R002C01SPC102 might allow remote attackers to execute arbitrary code with root Gain Privilegesileges via a crafted UDS patch with shell scripts. **CVE ID: CVE-2015-2252**	http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-417837.htm	O-HUA-OCEAN-210617/327
S5300 Firmware; S5700 Firmware; S6300 Firmware; S6700 Firmware; S7700 Firmware; S9300 Firmware; S9700 Firmware					
DoS	08-06-2017	7.8	The user authentication module in Huawei Campus switches S5700, S5300, S6300, and S6700 with software before V200R001SPH012 and S7700, S9300, and S9700 with software before V200R001SPH015 allows remote attackers to cause a denial of service (device restart) via vectors involving authentication, which trigger an array access violation. **CVE ID: CVE-2015-2800**	http://www.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-418554.htm	O-HUA-S5300-210617/328
Iodata					
Ts-wrla Firmware;Ts-wrlp Firmware					
Gain Information	09-06-2017	5	I-O DATA DEVICE TS-WRLP firmware version 1.00.01 and earlier and TS-WRLA firmware version 1.00.01 and earlier allow remote attackers to obtain	http://www.iodata.jp/support/information/2016/ts-wrlap/	O-IOD-TS-WR-210617/329

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

			authentication credentials via unspecified vectors. **CVE ID: CVE-2016-7814**		
Execute Code Overflow	09-06-2017	9	Buffer overflow in I-O DATA DEVICE TS-WRLP firmware version 1.01.02 and earlier and TS-WRLA firmware version 1.01.02 and earlier allows an attacker with administrator rights to cause a denial-of-service (DoS) or execute arbitrary code via unspecified vectors. **CVE ID: CVE-2016-7820**	http://www.iodata.jp/support/information/2016/ts-wrlap_2/	O-IOD-TS-WR-210617/330
Execute Code	09-06-2017	9	I-O DATA DEVICE TS-WRLP firmware version 1.01.02 and earlier and TS-WRLA firmware version 1.01.02 and earlier allows an attacker with administrator rights to execute arbitrary OS commands via unspecified vectors. **CVE ID: CVE-2016-7819**	http://www.iodata.jp/support/information/2016/ts-wrlap_2/	O-IOD-TS-WR-210617/331
Wfs-sr01 Firmware					
Bypass	09-06-2017	5	I-O DATA DEVICE WFS-SR01 firmware version 1.10 and earlier allow remote attackers to bypass access restriction to access data on storage devices inserted into the product via unspecified vectors. **CVE ID: CVE-2016-7807**	http://www.iodata.jp/support/information/2016/wfs-sr01/	O-IOD-WFS-S-210617/332
Execute Code	09-06-2017	10	I-O DATA DEVICE WFS-SR01 firmware version 1.10 and earlier allow remote attackers to execute arbitrary OS commands via unspecified vectors. **CVE ID: CVE-2016-7806**	http://www.iodata.jp/support/information/2016/wfs-sr01/	O-IOD-WFS-S-210617/333
Linux					
Linux Kernel					
Execute Code	14-06-2017	9.3	An elevation of Gain Privilegesilege vulnerability in the kernel FIQ debugger could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as	https://source.android.com/security/bulletin/2017-06-01	O-LIN-LINUX-210617/334

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

			High due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10. Android ID: A-36101220. **CVE ID: CVE-2017-0648**		
Paloaltonetworks					
Pan-os					
Execute Code	01-06-2017	9.3	Palo Alto Networks Panorama VM Appliance with PAN-OS before 6.0.1 might allow remote attackers to execute arbitrary Python code via a crafted firmware image file. **CVE ID: CVE-2015-6531**	NA	O-PAL-PAN-O-210617/335
Peplink					
1350hw2 Firmware; 2500 Firmware; 380hw6 Firmware; 580hw2 Firmware; 710hw3 Firmware; B305hw2 Firmware					
XSS	05-06-2017	4.3	XSS via orig_url exists on Peplink Balance 305, 380, 580, 710, 1350, and 2500 devices with firmware before fw-b305hw2_380hw6_580hw2_710hw3_1350hw2_2500-7.0.1-build2093. The affected script is guest/preview.cgi. **CVE ID: CVE-2017-8839**	NA	O-PEP-1350H-210617/336
XSS	05-06-2017	4.3	XSS via syncid exists on Peplink Balance 305, 380, 580, 710, 1350, and 2500 devices with firmware before fw-b305hw2_380hw6_580hw2_710hw3_1350hw2_2500-7.0.1-build2093. The affected script is cgi-bin/HASync/hasync.cgi. **CVE ID: CVE-2017-8838**	NA	O-PEP-1350H-210617/337
Gain Information	05-06-2017	5	Debug information disclosure exists on Peplink Balance 305, 380, 580, 710, 1350, and 2500 devices with firmware before fw-b305hw2_380hw6_580hw2_710hw3_1350hw2_2500-7.0.1-	NA	O-PEP-1350H-210617/338

			build2093. A direct request to cgi-bin/HASync/hasync.cgi?debug=1 shows Master LAN Address, Serial Number, HA Group ID, Virtual IP, and Submitted syncid. **CVE ID: CVE-2017-8840**		
NA	05-06-2017	5	Cleartext password storage exists on Peplink Balance 305, 380, 580, 710, 1350, and 2500 devices with firmware before fw-b305hw2_380hw6_580hw2_710hw3_1350hw2_2500-7.0.1-build2093. The files in question are /etc/waipass and /etc/roapass. In case one of these devices is compromised, the attacker can gain access to passwords and abuse them to compromise further systems. **CVE ID: CVE-2017-8837**	NA	O-PEP-1350H-210617/339
Execute Code; CSRF	05-06-2017	6.8	CSRF exists on Peplink Balance 305, 380, 580, 710, 1350, and 2500 devices with firmware before fw-b305hw2_380hw6_580hw2_710hw3_1350hw2_2500-7.0.1-build2093. The CGI scripts in the administrative interface are affected. This allows an attacker to execute commands, if a logged in user visits a malicious website. This can for example be used to change the credentials of the administrative webinterface. **CVE ID: CVE-2017-8836**	NA	O-PEP-1350H-210617/340
Directory Traversal	05-06-2017	7.5	Arbitrary file deletion exists on Peplink Balance 305, 380, 580, 710, 1350, and 2500 devices with firmware before fw-b305hw2_380hw6_580hw2_710hw3_1350hw2_2500-7.0.1-build2093. The attack methodology is absolute path traversal in cgi-bin/MANGA/firmware_process.cgi via the upfile.path parameter.	NA	O-PEP-1350H-210617/341

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

			CVE ID: CVE-2017-8841		
Sql	05-06-2017	7.5	SQL injection exists on Peplink Balance 305, 380, 580, 710, 1350, and 2500 devices with firmware before fw-b305hw2_380hw6_580hw2_710hw3_1350hw2_2500-7.0.1-build2093. An attack vector is the bauth cookie to cgi-bin/MANGA/admin.cgi. One impact is enumeration of user accounts by observing whether a session ID can be retrieved from the sessions database. **CVE ID: CVE-2017-8835**	NA	O-PEP-1350H-210617/342
Phoenixbroadband					
Poweragent Sc3 Bms Firmware					
NA	02-06-2017	5	A Use of Hard-Coded Password issue was discovered in Phoenix Broadband PowerAgent SC3 BMS, all versions prior to v6.87. Use of a hard-coded password may allow unauthorized access to the device. **CVE ID: CVE-2017-6039**	NA	O-PHO-POWER-210617/343
Redhat					
Enterprise Linux Desktop; Enterprise Linux Hpc Node; Enterprise Linux Server; Enterprise Linux Workstation					
info	08-06-2017	5	389 Directory Server in Red Hat Enterprise Linux Desktop 6 through 7, Red Hat Enterprise Linux HPC Node 6 through 7, Red Hat Enterprise Linux Server 6 through 7, and Red Hat Enterprise Linux Workstation 6 through 7 allows remote attackers to read the default Access Control Instructions. **CVE ID: CVE-2016-5416**	https://bugzilla.redhat.com/show_bug.cgi?id=1349540	O-RED-ENTER-210617/344
NA	08-06-2017	5	389 Directory Server in Red Hat Enterprise Linux Desktop 6 through 7, Red Hat Enterprise Linux HPC Node 6 through 7, Red Hat Enterprise Linux Server 6 through 7, and Red Hat Enterprise	https://bugzilla.redhat.com/show_bug.cgi?id=1358865	O-RED-ENTER-210617/345

			Linux Workstation 6 through 7 allows remote attackers to obtain user passwords. **CVE ID: CVE-2016-5405**		
Gain Information	08-06-2017	5	389 Directory Server in Red Hat Enterprise Linux Desktop 6 through 7, Red Hat Enterprise Linux HPC Node 6 through 7, Red Hat Enterprise Linux Server 6 through 7, and Red Hat Enterprise Linux Workstation 6 through 7 allows remote attackers to infer the existence of RDN component objects. **CVE ID: CVE-2016-4992**	https://bugzilla.redhat.com/show_bug.cgi?id=1347760	O-RED-ENTER-210617/346
NA	08-06-2017	5	mod_ns in Red Hat Enterprise Linux Desktop 7, Red Hat Enterprise Linux HPC Node 7, Red Hat Enterprise Linux Server 7, and Red Hat Enterprise Linux Workstation 7 allows remote attackers to force the use of ciphers that were not intended to be enabled. **CVE ID: CVE-2016-3099**	https://bugzilla.redhat.com/show_bug.cgi?id=1319052	O-RED-ENTER-210617/347
Execute Code	08-06-2017	7.5	SerializableProvider in RESTEasy in Red Hat Enterprise Linux Desktop 7, Red Hat Enterprise Linux HPC Node 7, Red Hat Enterprise Linux Server 7, and Red Hat Enterprise Linux Workstation 7 allows remote attackers to execute arbitrary code. **CVE ID: CVE-2016-7050**	https://bugzilla.redhat.com/show_bug.cgi?id=1378613	O-RED-ENTER-210617/348
Samsung					
Galaxy S6 Edge Firmware					
Directory Traversal	07-06-2017	7.8	Directory traversal vulnerability in the WifiHs20UtilityService on the Samsung S6 Edge LRX22G.G925VVRU1AOE2 allows remote attackers to overwrite or create arbitrary files as the system-level user via a .. (dot dot) in the name of a file, compressed into a	NA	O-SAM-GALAX-210617/349

			zipped file named cred.zip, and downloaded to /sdcard/Download. **CVE ID: CVE-2015-7888**		
Seagate					
Business Nas Firmware					
Execute Code	08-06-2017	10	Seagate Business NAS devices with firmware before 2015.00322 allow remote attackers to execute arbitrary code with root Gain Privilegesileges by leveraging use of a static encryption key to create session tokens. **CVE ID: CVE-2014-8687**	NA	O-SEA-BUSIN-210617/350
Sophos					
Cyberoam Firmware					
XSS	07-06-2017	4.3	An XSS vulnerability allows remote attackers to execute arbitrary client side script on vulnerable installations of Sophos Cyberoam firewall devices with firmware through 10.6.4. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of a request to the "LiveConnectionDetail.jsp" application. GET parameters "applicationname" and "username" are improperly sanitized allowing an attacker to inject arbitrary JavaScript into the page. This can be abused by an attacker to perform a cross-site scripting attack on the user. A vulnerable URI is /corporate/webpages/trafficdiscovery/LiveConnectionDetail.jsp. **CVE ID: CVE-2016-9834**	http://seclists.org/bugtraq/2017/Jun/4	O-SOP-CYBER-210617/351

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