National Critical Information Infrastructure Protection Center

CVE Report

16- 29 May 2016 Vol.03 No.09

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Application					
Apache					
Ambari *The Apache Ambari project is aimed at making Hadoop management simpler by developing software for provisioning, managing, and monitoring Apache Hadoop clusters*					
Gain Info	2016-05-18	4	The File Browser View in Apache Ambari before 2.2.1 allows remote authenticated administrators to read arbitrary files via a file: URL in the WebHDFS URL configuration. **Reference: CVE-2016-0731**	https://cwiki.apache.org/confluence/display/AMBARI/Ambari+Vulnerabilities#AmbariVulnerabilities-FixedinAmbari2.2.1	A-APA-AMBAR-20616/1
Gain Information	2016-05-18	2.1	The agent in Apache Ambari before 2.1.2 uses weak permissions for the (1) /var/lib/ambari-agent/data and (2) /var/lib/ambari-agent/keys directories, which allows local users to obtain sensitive information by reading files in the directories. **Reference: CVE-2016-0707**	https://cwiki.apache.org/confluence/display/AMBARI/Ambari+Vulnerabilities#AmbariVulnerabilities-FixedinAmbari2.1.2	A-APA-AMBAR-20616/2
Apple					
Itunes *iTunes is a free application for Mac and PC. It plays all your digital music and video.*					
Gain Privileges	2016-05-20	7.2	Untrusted search path vulnerability in the installer in Apple iTunes before 12.4 allows local users to gain privileges via a Trojan horse DLL in the current working directory. **Reference : CVE-2016-1742**	https://support.apple.com/HT206379	A-APP-ITUNE-20616/3

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

Cisco

Adaptive Security Appliance Firmware: *Cisco ASA Software delivers enterprise-class security capabilities for the ASA security family in a variety of form factors.*

Denial of Service Overflow	2016-05-26	6.8	The XML parser in Cisco Adaptive Security Appliance (ASA) Software through 9.5.2 allows remote authenticated users to cause a denial of service (instability, memory consumption, or device reload) by leveraging (1) administrative access or (2) Clientless SSL VPN access to provide a crafted XML document, aka Bug ID CSCut14209. **Reference : CVE-2016-1385**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160517-asa-xml	A-CIS-ADAPT-20616/4

Evolved Programmable Network Manager; Prime Infrastructure: *Cisco Evolved Programmable Network Manager provides simplified, converged, multilayer management of carrier-grade networks of all sizes.*

Gain Privileges Bypass Gain Info	2016-05-24	6.5	The API web interface in Cisco Prime Infrastructure before 3.1 and Cisco Evolved Programmable Network Manager before 1.2.4 allows remote authenticated users to bypass intended RBAC restrictions and obtain sensitive information, and consequently gain privileges, via crafted JSON data, aka Bug ID CSCuy12409. **Reference : CVE-2016-1406**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160523-pi-epnm	A-CIS-EVOLV-20616/5

Identity Services Engine Software: *ISE is a policy management and control platform for wired, wireless, and VPN.*

Denial of Service Overflow	2016-05-20	5	The Active Directory (AD) integration component in Cisco Identity Service Engine (ISE) before 1.2.0.899 patch 7, when AD group-membership authorization is enabled, allows remote attackers to cause a denial of service (authentication outage) via	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160517-ise	A-CIS-IDENT-20616/6

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

			a crafted Password Authentication Protocol (PAP) authentication request, aka Bug ID CSCun25815. **Reference : CVE-2016-1402**		
Telepresence Video Communication Server: *The Cisco TelePresence Video Communication Server simplifies session management and control of telepresence conferences*					
Denial of Service	2016-05-24	5	Cisco TelePresence Video Communications Server (VCS) X8.x before X8.7.2 allows remote attackers to cause a denial of service (service disruption) via a crafted URI in a SIP header, aka Bug ID CSCuy43258. **Reference : CVE-2016-1400**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160516-vcs	A-CIS-TELEP-20616/7
Unified Computing System: *The Cisco Unified Computing System (UCS) is an (x86) architecture data center server platform composed of computing hardware, virtualization support, switching fabric, and management software introduced in 2009.*					
XSS	2016-05-20	4.3	Cross-site scripting (XSS) vulnerability in the management interface in Cisco Unified Computing System (UCS) Central Software 1.4(1a) allows remote attackers to inject arbitrary web script or HTML via a crafted value, aka Bug ID CSCuy91250. **Reference : CVE-2016-1401**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160517-ucs	A-CIS-UNIFI-20616/8
Web Security Appliance: *Cisco Web Security Appliance provides exceptional web security and control for organizations of all sizes – integrated into one appliance.*					
Denial of Service	2016-05-24	7.8	Memory leak in Cisco AsyncOS 8.5 through 9.0 before 9.0.1-162 on Web Security Appliance (WSA) devices allows remote attackers to cause a denial of service (memory consumption) via an HTTP file-range request for cached content, aka Bug ID CSCuw97270. **Reference : CVE-2016-**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160518-wsa2	A-CIS-WEB S-20616/9

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

			1381		
Denial of Service	2016-05-24	7.8	Cisco AsyncOS 8.0 before 8.0.6-119 on Web Security Appliance (WSA) devices allows remote attackers to cause a denial of service (proxy-process hang) via a crafted HTTP POST request, aka Bug ID CSCuo12171. **Reference : CVE-2016-1380**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160518-wsa1	A-CIS-WEB S-20616/10
Denial of Service	2016-05-24	7.8	Memory leak in Cisco AsyncOS through 8.8 on Web Security Appliance (WSA) devices allows remote attackers to cause a denial of service (memory consumption) via an unspecified HTTP status code, aka Bug ID CSCur28305. **Reference : CVE-2016-1383**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160518-wsa4	A-CIS-WEB S-20616/11
Denial of Service	2016-05-24	7.8	Cisco AsyncOS before 8.5.3-069 and 8.6 through 8.8 on Web Security Appliance (WSA) devices mishandles memory allocation for HTTP requests, which allows remote attackers to cause a denial of service (proxy-process reload) via a crafted request, aka Bug ID CSCuu02529. **Reference : CVE-2016-1382**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160518-wsa3	A-CIS-WEB S-20616/12
Cloudbees					
Jenkins: *Jenkins is a self-contained Java-based program, ready to run out-of-the-box, with packages for Windows, Mac OS X and other Unix-like operating systems.*					
Gain Info	2016-05-17	4	The API URL computer/(master)/api/xml in CloudBees Jenkins before 2.3 and LTS before 1.651.2 allows remote authenticated users with extended read permission for the master node to obtain sensitive information about the global configuration via	https://www.cloudbees.com/jenkins-security-advisory-2016-05-11	A-CLO-JENKI-20616/13

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

			unspecified vectors. **Reference : CVE-2016-3727**		
	2016-05-17	5.8	Multiple open redirect vulnerabilities in CloudBees Jenkins before 2.3 and LTS before 1.651.2 allow remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors related to "scheme-relative" URLs. **Reference : CVE-2016-3726**	https://www.cloudbees.com/jenkins-security-advisory-2016-05-11	A-CLO-JENKI-20616/14
Denial of Service	2016-05-17	5	CloudBees Jenkins before 2.3 and LTS before 1.651.2 allows remote authenticated users to trigger updating of update site metadata by leveraging a missing permissions check. NOTE: this issue can be combined with DNS cache poisoning to cause a denial of service (service disruption). **Reference : CVE-2016-3725**	https://www.cloudbees.com/jenkins-security-advisory-2016-05-11	A-CLO-JENKI-20616/15
Gain Info	2016-05-17	4	CloudBees Jenkins before 2.3 and LTS before 1.651.2 allow remote authenticated users with extended read access to obtain sensitive password information by reading a job configuration. **Reference : CVE-2016-3724**	https://www.cloudbees.com/jenkins-security-advisory-2016-05-11	A-CLO-JENKI-20616/16
Gain Info	2016-05-17	4	CloudBees Jenkins before 2.3 and LTS before 1.651.2 allow remote authenticated users with read access to obtain sensitive plugin installation information by leveraging missing permissions checks in unspecified XML/JSON API endpoints. **Reference : CVE-2016-3723**	https://www.cloudbees.com/jenkins-security-advisory-2016-05-11	A-CLO-JENKI-20616/17

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

Denial of Service	2016-05-17	4	CloudBees Jenkins before 2.3 and LTS before 1.651.2 allow remote authenticated users with multiple accounts to cause a denial of service (unable to login) by editing the "full name." **Reference : CVE-2016-3722**	https://www.cloudbees.com/jenkins-security-advisory-2016-05-11	A-CLO-JENKI-20616/18
	2016-05-17	4	CloudBees Jenkins before 2.3 and LTS before 1.651.2 might allow remote authenticated users to inject arbitrary build parameters into the build environment via environment variables. **Reference : CVE-2016-3721**	https://wiki.jenkins-ci.org/display/JENKINS/Plugins+affected+by+fix+for+SECURITY-170	A-CLO-JENKI-20616/19
Cmsmadesimple					
Cms Made Simple: *CMS Made Simple (CMSMS) is a free, open source (GPL) content management system (CMS) to provide developers, programmers and site owners a web-based development and administration area.*					
XSS	2016-05-26	2.6	CMS Made Simple 2.x before 2.1.3 and 1.x before 1.12.2, when Smarty Cache is activated, allow remote attackers to conduct cache poisoning attacks, modify links, and conduct cross-site scripting (XSS) attacks via a crafted HTTP Host header in a request. **Reference : CVE-2016-2784**	http://www.cmsmadesimple.org/2016/03/Announcing-CMSMS-1-12-2-kolonia/	A-CMS-CMS M-20616/20
Gnome					
Librsvg: *librsvg is a free software SVG rendering library written as part of the GNOME project, intended to be lightweight and portable.*					
Denial of Service	2016-05-20	5	librsvg before 2.40.12 allows context-dependent attackers to cause a denial of service (infinite loop, stack consumption, and application crash) via cyclic references in an SVG document. **Reference : CVE-2015-7558**	https://bugzilla.redhat.com/show_bug.cgi?id=1268243	A-GNO-LIBRS-20616/21

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

Denial of Service	2016-05-20	5	The _rsvg_node_poly_build_path function in rsvg-shapes.c in librsvg before 2.40.7 allows context-dependent attackers to cause a denial of service (out-of-bounds heap read) via an odd number of elements in a coordinate pair in an SVG document. **Reference : CVE-2015-7557**	https://git.gnome.org/browse/librsvg/tree/NEWS	A-GNO-LIBRS-20616/22
Golang					
GO: *Go is an open source programming language created at Google in 2007*					
Gain Privileges	2016-05-23	7.2	Untrusted search path vulnerability in Go before 1.5.4 and 1.6.x before 1.6.1 on Windows allows local users to gain privileges via a Trojan horse DLL in the current working directory, related to use of the LoadLibrary function. **Reference : CVE-2016-3958**	https://github.com/golang/go/issues/14959	A-GOL-GO-20616/23
Haxx					
Curl: *Computer software project providing a library and command-line tool for transferring data using various protocols.*					
	2016-05-20	2.6	The (1) mbed_connect_step1 function in lib/vtls/mbedtls.c and (2) polarssl_connect_step1 function in lib/vtls/polarssl.c in cURL and libcurl before 7.49.0, when using SSLv3 or making a TLS connection to a URL that uses a numerical IP address, allow remote attackers to spoof servers via an arbitrary valid certificate. **Reference : CVE-2016-3739**	https://curl.haxx.se/changes.html#7_49_0	A-HAX-CURL-20616/23
Hhvm/PHP					
Hhvm/PHP: *HHVM is an open-source virtual machine designed for executing programs written in Hack and PHP. PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language.*					

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

Dir. Trav.	2016-05-21	4.3	Directory traversal vulnerability in the ZipArchive::extractTo function in ext/zip/php_zip.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 and ext/zip/ext_zip.cpp in HHVM before 3.12.1 allows remote attackers to create arbitrary empty directories via a crafted ZIP archive. **Reference : CVE-2014-9767**	http://php.net/ChangeLog-5.php	A-HHV-HHVM/-20616/24
Huawei					
Mobile Broadband Hl Service: *Mobile Broadband HL Service is a software program developed by Huawei Technologies Co.,Ltd.*					
Gain Priv	2016-05-23	7.2	The Huawei Mobile Broadband HL Service 22.001.25.00.03 and earlier uses a weak ACL for the MobileBrServ program data directory, which allows local users to gain SYSTEM privileges by modifying VERSION.dll. **Reference : CVE-2016-2855**		A-HUA-MOBIL-20616/25
IBM					
Bluemix: *Bluemix is an open standards, cloud platform for building, running, and managing apps and services*					
Bypass	2016-05-17	4	The Auto-Scaling agent in Liberty for Java in IBM Bluemix before 2.7-20160321-1358 allows remote authenticated users to disable X.509 certificate validation, and consequently bypass an intended HTTPS trust-management feature, via unspecified vectors. **Reference : CVE-2016-0323**	http://www-01.ibm.com/support/docview.wss?uid=swg21979682	A-IBM-BLUEM-20616/26
Websphere Application Server: *WebSphere Application Server (WAS) is a software product that performs the role of a web application server. More specifically, it is a software framework and middleware that hosts Java based web applications. It is the flagship product within IBM's WebSphere software suite.*					

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

Gain Info	2016-05-17	4.3	IBM WebSphere Application Server (WAS) 7.0 before 7.0.0.41, 8.0 before 8.0.0.13, and 8.5 before 8.5.5.10, when FIPS 140-2 is enabled, misconfigures TLS, which allows man-in-the-middle attackers to obtain sensitive information via unspecified vectors. **Reference : CVE-2016-0306**	http://www-01.ibm.com/support/docview.wss?uid=swg21979231	A-IBM-WEBSP-20616/27
Jansson Project					
Jansson: *Jansson is a C library for encoding, decoding and manipulating JSON data.*					
Denial of Service	2016-05-17	5	Jansson 2.7 and earlier allows context-dependent attackers to cause a denial of service (deep recursion, stack consumption, and crash) via crafted JSON data. **Reference : CVE-2016-4425**	https://github.com/akheron/jansson/issues/282	A-JAN-JANSS-20616/28
Lenovo					
Shareit: *SHAREit is a FREE file sharing app that works across multiple operating systems.*					
XSS	2016-05-23	4.3	Cross-site scripting (XSS) vulnerability in Lenovo SHAREit before 3.5.98_ww on Android before 4.4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Universal XSS (UXSS)." **Reference : CVE-2016-4783**	https://support.lenovo.com/us/en/product_security/len_6421	A-LEN-SHARE-20616/29
	2016-05-23	9.3	Lenovo SHAREit before 3.5.98_ww on Android before 4.2 allows remote attackers to have unspecified impact via a crafted intent: URL, aka an "intent scheme URL attack." **Reference : CVE-2016-4782**	https://support.lenovo.com/us/en/product_security/len_6421	A-LEN-SHARE-20616/30
Libgd;PHP					

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

Libgd/PHP: *PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language. GD is an open source code library for the dynamic creation of images by programmers.*					
Denial of Service	2016-05-21	5	The gdImageScaleTwoPass function in gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.2.0, as used in PHP before 5.6.12, uses inconsistent allocate and free approaches, which allows remote attackers to cause a denial of service (memory consumption) via a crafted call, as demonstrated by a call to the PHP imagescale function. **Reference : CVE-2015-8877**	http://www.php.net/ChangeLog-5.php	A-LIB-LIBGD-20616/31
Mariadb;Oracle					
Mariadb/Mysql;Mysql Connector C: *MariaDB is a community-developed fork of the MySQL relational database management system intended to remain free under the GNU GPL. MySQL is an open-source relational database management system (RDBMS). MySQL Connector/C is a client library that implements the C API for client/server communication.*					
	2016-05-16	4.3	Oracle MySQL before 5.7.3, Oracle MySQL Connector/C (aka libmysqlclient) before 6.1.3, and MariaDB before 5.5.44 use the --ssl option to mean that SSL is optional, which allows man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack, aka a "BACKRONYM" attack. **Reference : CVE-2015-3152**	https://access.redhat.com/security/cve/cve-2015-3152	A-MAR-MARIA-20616/32
Mediaelementjs;Wordpress					
Mediaelement.js/Wordpress: *MediaElement.js is free and open source HTML5 video player built by John Dyer. WordPress is web software you can use to create a beautiful website, blog, or app.*					
XSS	2016-05-21	4.3	Cross-site scripting (XSS) vulnerability in flash/FlashMediaElement.as in MediaElement.js before 2.21.0, as used in WordPress before 4.5.2,	https://codex.wordpress.org/Version_4.5.2	A-MED-MEDIA-20616/33

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

			allows remote attackers to inject arbitrary web script or HTML via the query string. **Reference : CVE-2016-4567**		
Moodle					
Moodle: *Moodle is a free and open-source software learning management system written in PHP and distributed under the GNU General Public License.*					
Gain Info	2016-05-22	5	Moodle through 2.6.11, 2.7.x before 2.7.13, 2.8.x before 2.8.11, 2.9.x before 2.9.5, and 3.0.x before 3.0.3 does not properly restrict links, which allows remote attackers to obtain sensitive URL information by reading a Referer log. **Reference : CVE-2016-2190**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-52651	A-MOO-MOODL-20616/34
Bypass	2016-05-22	4	The save_submission function in mod/assign/externallib.php in Moodle through 2.6.11, 2.7.x before 2.7.13, 2.8.x before 2.8.11, 2.9.x before 2.9.5, and 3.0.x before 3.0.3 allows remote authenticated users to bypass intended due-date restrictions by leveraging the student role for a web-service request. **Reference : CVE-2016-2159**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-52901	A-MOO-MOODL-20616/35
Gain Info	2016-05-22	4	lib/ajax/getnavbranch.php in Moodle through 2.6.11, 2.7.x before 2.7.13, 2.8.x before 2.8.11, 2.9.x before 2.9.5, and 3.0.x before 3.0.3, when the forcelogin feature is enabled, allows remote attackers to obtain sensitive category-detail information from the navigation branch by leveraging the guest role for an Ajax request. **Reference : CVE-2016-2158**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-52774	A-MOO-MOODL-20616/36

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

CSRF	2016-05-22	6.8	Cross-site request forgery (CSRF) vulnerability in mod/assign/adminmanagep lugins.php in Moodle through 2.6.11, 2.7.x before 2.7.13, 2.8.x before 2.8.11, 2.9.x before 2.9.5, and 3.0.x before 3.0.3 allows remote attackers to hijack the authentication of administrators for requests that manage Assignment plugins. **Reference : CVE-2016-2157**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-53031	A-MOO-MOODL-20616/37
Gain Info	2016-05-22	4	calendar/externallib.php in Moodle through 2.6.11, 2.7.x before 2.7.13, 2.8.x before 2.8.11, 2.9.x before 2.9.5, and 3.0.x before 3.0.3 provides calendar-event data without considering whether an activity is hidden, which allows remote authenticated users to obtain sensitive information via a web-service request. **Reference : CVE-2016-2156**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-52808	A-MOO-MOODL-20616/38
	2016-05-22	4	The grade-reporting feature in Singleview (aka Single View) in Moodle 2.8.x before 2.8.11, 2.9.x before 2.9.5, and 3.0.x before 3.0.3 does not consider the moodle/grade:manage capability, which allows remote authenticated users to modify "Exclude grade" settings by leveraging the Non-Editing Instructor role. **Reference : CVE-2016-2155**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-52378	A-MOO-MOODL-20616/39
Gain Info	2016-05-22	4	admin/tool/monitor/lib.php in Event Monitor in Moodle 2.8.x before 2.8.11, 2.9.x before 2.9.5, and 3.0.x before 3.0.3 does not consider the	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=M	A-MOO-MOODL-20616/40

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

			moodle/course:viewhiddencourses capability, which allows remote authenticated users to discover hidden course names by subscribing to a rule. **Reference : CVE-2016-2154**	DL-51167	
XSS	2016-05-22	4.3	Cross-site scripting (XSS) vulnerability in the advanced-search feature in mod_data in Moodle through 2.6.11, 2.7.x before 2.7.13, 2.8.x before 2.8.11, 2.9.x before 2.9.5, and 3.0.x before 3.0.3 allows remote attackers to inject arbitrary web script or HTML via a crafted field in a URL, as demonstrated by a search form field. **Reference : CVE-2016-2153**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-52727	A-MOO-MOODL-20616/41
XSS	2016-05-22	4.3	Multiple cross-site scripting (XSS) vulnerabilities in auth/db/auth.php in Moodle through 2.6.11, 2.7.x before 2.7.13, 2.8.x before 2.8.11, 2.9.x before 2.9.5, and 3.0.x before 3.0.3 allow remote attackers to inject arbitrary web script or HTML via an external DB profile field. **Reference : CVE-2016-2152**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-50705	A-MOO-MOODL-20616/42
Gain Info	2016-05-22	4	user/index.php in Moodle through 2.6.11, 2.7.x before 2.7.13, 2.8.x before 2.8.11, 2.9.x before 2.9.5, and 3.0.x before 3.0.3 grants excessive authorization on the basis of the moodle/course:viewhiddenuserfields capability, which allows remote authenticated users to discover student e-mail addresses by leveraging	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-52433	A-MOO-MOODL-20616/43

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

			the teacher role and reading a Participants list. **Reference : CVE-2016-2151**		
PHP					
PHP: *PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language.*					
Denial of Service Gain Info	2016-05-16	6.4	The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, 5.6.x before 5.6.12, and 7.x before 7.0.4 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (type confusion and application crash) via crafted serialized _cookies data, related to the SoapClient::__call method in ext/soap/soap.c. **Reference : CVE-2016-3185**	http://php.net/ChangeLog-7.php	A-PHP-PHP-20616/44
Denial of Service Overflow	2016-05-16	10	Stack-based buffer overflow in ext/phar/tar.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted TAR archive. **Reference : CVE-2016-2554**	https://bugs.php.net/bug.php?id=71488	A-PHP-PHP-20616/45
Denial of Service Overflow	2016-05-16	5	Stack consumption vulnerability in GD in PHP before 5.6.12 allows remote attackers to cause a denial of service via a crafted imagefilltoborder call. **Reference : CVE-2015-8874**	https://bugs.php.net/bug.php?id=66387	A-PHP-PHP-20616/46
Denial of Service	2016-05-16	5	Stack consumption vulnerability in Zend/zend_exceptions.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x	https://bugs.php.net/bug.php?id=69793	A-PHP-PHP-20616/47

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

			before 5.6.12 allows remote attackers to cause a denial of service (segmentation fault) via recursive method calls. **Reference : CVE-2015-8873**		
	2016-05-16	4.3	ext/mysqlnd/mysqlnd.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 uses a client SSL option to mean that SSL is optional, which allows man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack, a related issue to CVE-2015-3152. **Reference : CVE-2015-8838**	https://bugs.php.net/bug.php?id=69669	A-PHP-PHP-20616/48
Denial of Service Exec Code	2016-05-16	7.5	The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not properly retrieve keys, which allows remote attackers to cause a denial of service (NULL pointer dereference, type confusion, and application crash) or possibly execute arbitrary code via crafted serialized data representing a numerically indexed _cookies array, related to the SoapClient::__call method in ext/soap/soap.c. **Reference : CVE-2015-8835**	http://php.net/ChangeLog-5.php	A-PHP-PHP-20616/49
Denial of Service Exec Code	2016-05-16	7.5	The session deserializer in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 mishandles multiple php_var_unserialize calls, which allow remote attackers to execute arbitrary code or cause a	http://php.net/ChangeLog-5.php	A-PHP-PHP-20616/50

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

			denial of service (use-after-free) via crafted session content. **Reference : CVE-2015-6835**		
Exec Code	2016-05-16	7.5	Multiple use-after-free vulnerabilities in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 allow remote attackers to execute arbitrary code via vectors related to (1) the Serializable interface, (2) the SplObjectStorage class, and (3) the SplDoublyLinkedList class, which are mishandled during unserialization. **Reference : CVE-2015-6834**	http://php.net/ChangeLog-5.php	A-PHP-PHP-20616/51
Denial of Service	2016-05-16	10	The phar_convert_to_other function in ext/phar/phar_object.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 does not validate a file pointer before a close operation, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted TAR archive that is mishandled in a Phar::convertToData call. **Reference : CVE-2015-5589**	https://bugs.php.net/bug.php?id=69958	A-PHP-PHP-20616/52
Denial of Service	2016-05-16	5	The php_pgsql_meta_data function in pgsql.c in the PostgreSQL (aka pgsql) extension in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not validate token extraction for table names, which might allow remote attackers to cause a denial of service (NULL pointer dereference and application	http://git.php.net/?p=php-src.git;a=commit;h=2cc4e69cc6d8dbc4b3568ad3dd583324a7c11d64	A-PHP-PHP-20616/53

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

			crash) via a crafted name. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-1352. **Reference : CVE-2015-4644**		
Exec Code Overflow	2016-05-16	7.5	Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-4022. **Reference : CVE-2015-4643**	http://git.php.net/?p=php-src.git;a=commit;h=0765623d6991b62ffcd93ddb6be8a5203a2fa7e2	A-PHP-PHP-20616/54
Exec Code	2016-05-16	10	The escapeshellarg function in ext/standard/exec.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Windows allows remote attackers to execute arbitrary OS commands via a crafted string to an application that accepts command-line arguments for a call to the PHP system function. **Reference : CVE-2015-4642**	http://git.php.net/?p=php-src.git;a=commit;h=d2ac264ffea5ca2e85640b6736e0c7cd4ee9a4a9	A-PHP-PHP-20616/55
Denial of Service Exec Code	2016-05-16	5	The mcopy function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly restrict a certain offset value, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string	https://bugs.php.net/bug.php?id=68819	A-PHP-PHP-20616/56

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

			that is mishandled by a "Python script text executable" rule. **Reference : CVE-2015-4605**		
Denial of Service Exec Code	2016-05-16	5	The mget function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly maintain a certain pointer relationship, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string that is mishandled by a "Python script text executable" rule. **Reference : CVE-2015-4604**	http://php.net/ChangeLog-5.php	A-PHP-PHP-20616/57
Exec Code	2016-05-16	10	The exception::getTraceAsString function in Zend/zend_exceptions.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to execute arbitrary code via an unexpected data type, related to a "type confusion" issue. **Reference : CVE-2015-4603**	https://bugs.php.net/bug.php?id=69152	A-PHP-PHP-20616/58
Denial of Service Exec Code	2016-05-16	10	The __PHP_Incomplete_Class function in ext/standard/incomplete_class.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to a	https://bugs.php.net/bug.php?id=69152	A-PHP-PHP-20616/59

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

			"type confusion" issue. **Reference : CVE-2015-4602**		
Denial of Service Exec Code	2016-05-16	10	PHP before 5.6.7 might allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in (1) ext/soap/php_encoding.c, (2) ext/soap/php_http.c, and (3) ext/soap/soap.c, a different issue than CVE-2015-4600. **Reference : CVE-2015-4601**	http://git.php.net/?p=php-src.git;a=commit;h=0c136a2abd49298b66acb0cad504f0f972f5bfe8	A-PHP-PHP-20616/60
Denial of Service Exec Code	2016-05-16	10	The SoapClient implementation in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in the (1) SoapClient::__getLastRequest, (2) SoapClient::__getLastResponse, (3) SoapClient::__getLastRequestHeaders, (4) SoapClient::__getLastResponseHeaders, (5) SoapClient::__getCookies, and (6) SoapClient::__setCookie methods. **Reference : CVE-2015-4600**	https://bugs.php.net/bug.php?id=69152	A-PHP-PHP-20616/61
Denial of Service Exec Code Gain Info	2016-05-16	10	The SoapFault::__toString method in ext/soap/soap.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain	https://bugs.php.net/bug.php?id=69152	A-PHP-PHP-20616/62

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

			sensitive information, cause a denial of service (application crash), or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue. **Reference : CVE-2015-4599**		
Bypass	2016-05-16	7.5	PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument save method or (2) the GD imagepsloadfont function, as demonstrated by a filename\0.html attack that bypasses an intended configuration in which client users may write to only .html files. **Reference : CVE-2015-4598**	https://bugs.php.net/bug.php?id=69719	A-PHP-PHP-20616/63
Exec Code	2016-05-16	7.5	Use-after-free vulnerability in the spl_ptr_heap_insert function in ext/spl/spl_heap.c in PHP before 5.5.27 and 5.6.x before 5.6.11 allows remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation. **Reference : CVE-2015-4116**	http://git.php.net/?p=php-src.git;a=commit;h=1cbd25ca15383394ffa9ee8601c5de4c0f2f90e1	A-PHP-PHP-20616/64
Bypass	2016-05-16	5	PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read arbitrary files via crafted input to an	https://bugs.php.net/bug.php?id=69353	A-PHP-PHP-20616/65

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

			application that calls the stream_resolve_include_path function in ext/standard/streamsfuncs.c, as demonstrated by a filename\0.extension attack that bypasses an intended configuration in which client users may read files with only one specific extension. **Reference : CVE-2015-3412**		
Bypass	2016-05-16	6.4	PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument load method, (2) the xmlwriter_open_uri function, (3) the finfo_file function, or (4) the hash_hmac_file function, as demonstrated by a filename\0.xml attack that bypasses an intended configuration in which client users may read only .xml files. **Reference : CVE-2015-3411**	http://git.php.net/?p=php-src.git;a=commit;h=4435b9142ff9813845d5c97ab29a5d637bedb257	A-PHP-PHP-20616/66
Denial of Service	2016-05-16	5	file before 5.18, as used in the Fileinfo component in PHP before 5.6.0, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a zero root_storage value in a CDF file, related to cdf.c and readcdf.c. **Reference : CVE-2014-0236**	http://git.php.net/?p=php-src.git;a=commit;h=f3f22ff5c697aef854ffc1918bce708b37481b0f	A-PHP-PHP-20616/67
Denial of Service Overflow	2016-05-20	5	** DISPUTED ** Integer overflow in the php_raw_url_encode	https://git.php.net/?p=php-	A-PHP-PHP-20616/68

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

			function in ext/standard/url.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to cause a denial of service (application crash) via a long string to the rawurlencode function. NOTE: the vendor says "Not sure if this qualifies as security issue (probably not)." **Reference : CVE-2016-4070**	src.git;a=commit;h=95433e8e339dbb6b5d5541473c1661db6ba2c451	
Denial of Service Overflow	2016-05-21	7.5	The exif_process_TIFF_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate TIFF start data, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data. **Reference : CVE-2016-4544**	http://php.net/ChangeLog-5.php	A-PHP-PHP-20616/69
Denial of Service Overflow	2016-05-21	7.5	The exif_process_IFD_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate IFD sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data. **Reference : CVE-2016-4543**	http://php.net/ChangeLog-5.php	A-PHP-PHP-20616/70
Denial of Service	2016-05-21	7.5	The exif_process_IFD_TAG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x	http://php.net/ChangeLog-5.php	A-PHP-PHP-20616/71

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

			before 5.6.21, and 7.x before 7.0.6 does not properly construct spprintf arguments, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data. **Reference : CVE-2016-4542**		
Denial of Service	2016-05-21	7.5	The grapheme_strpos function in ext/intl/grapheme/grapheme_string.c in before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset. **Reference : CVE-2016-4541**	http://php.net/ChangeLog-5.php	A-PHP-PHP-20616/72
Denial of Service	2016-05-21	7.5	The grapheme_stripos function in ext/intl/grapheme/grapheme_string.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset. **Reference : CVE-2016-4540**	http://php.net/ChangeLog-5.php	A-PHP-PHP-20616/73
Denial of Service Overflow	2016-05-21	7.5	The xml_parse_into_struct function in ext/xml/xml.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (buffer under-read and segmentation fault) or possibly have unspecified other impact via crafted XML data in the	http://php.net/ChangeLog-5.php	A-PHP-PHP-20616/74

			second argument, leading to a parser level of zero. **Reference : CVE-2016-4539**		
Denial of Service	2016-05-21	7.5	The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 modifies certain data structures without considering whether they are copies of the _zero_, _one_, or _two_ global variable, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call. **Reference : CVE-2016-4538**	http://php.net/ChangeLog-5.php	A-PHP-PHP-20616/75
Denial of Service	2016-05-21	7.5	The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 accepts a negative integer for the scale argument, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call. **Reference : CVE-2016-4537**	http://php.net/ChangeLog-7.php	A-PHP-PHP-20616/76
Denial of Service Overflow	2016-05-21	7.5	Integer overflow in the str_pad function in ext/standard/string.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long string, leading to a heap-based buffer overflow. **Reference : CVE-2016-4346**	http://php.net/ChangeLog-7.php	A-PHP-PHP-20616/77
Denial of Service Overflow	2016-05-21	7.5	Integer overflow in the php_filter_encode_url function in	http://php.net/ChangeLog-7.php	A-PHP-PHP-20616/78

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

			ext/filter/sanitizing_filters.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long string, leading to a heap-based buffer overflow. **Reference : CVE-2016-4345**		
Denial of Service Overflow	2016-05-21	7.5	Integer overflow in the xml_utf8_encode function in ext/xml/xml.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long argument to the utf8_encode function, leading to a heap-based buffer overflow. **Reference : CVE-2016-4344**	http://php.net/ChangeLog-7.php	A-PHP-PHP-20616/79
Denial of Service	2016-05-21	6.8	The phar_make_dirstream function in ext/phar/dirstream.c in PHP before 5.6.18 and 7.x before 7.0.3 mishandles zero-size ./.@LongLink files, which allows remote attackers to cause a denial of service (uninitialized pointer dereference) or possibly have unspecified other impact via a crafted TAR archive. **Reference : CVE-2016-4343**	https://bugs.php.net/bug.php?id=71331	A-PHP-PHP-20616/80
Denial of Service Overflow Mem. Corr.	2016-05-21	8.3	ext/phar/phar_object.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 mishandles zero-length uncompressed data, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted (1) TAR, (2) ZIP, or (3) PHAR archive.	http://php.net/ChangeLog-5.php	A-PHP-PHP-20616/81

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

			Reference : CVE-2016-4342		
	2016-05-21	10	Double free vulnerability in the format printer in PHP 7.x before 7.0.1 allows remote attackers to have an unspecified impact by triggering an error. **Reference : CVE-2015-8880**	http://php.net/ChangeLog-7.php	A-PHP-PHP-20616/82
Denial of Service	2016-05-21	5	The odbc_bindcols function in ext/odbc/php_odbc.c in PHP before 5.6.12 mishandles driver behavior for SQL_WVARCHAR columns, which allows remote attackers to cause a denial of service (application crash) in opportunistic circumstances by leveraging use of the odbc_fetch_array function to access a certain type of Microsoft SQL Server table. **Reference : CVE-2015-8879**	https://bugs.php.net/bug.php?id=69975	A-PHP-PHP-20616/83
Denial of Service Overflow Mem. Corr.	2016-05-21	7.1	main/php_open_temporary_file.c in PHP before 5.5.28 and 5.6.x before 5.6.12 does not ensure thread safety, which allows remote attackers to cause a denial of service (race condition and heap memory corruption) by leveraging an application that performs many temporary-file accesses. **Reference : CVE-2015-8878**	https://bugs.php.net/bug.php?id=70002	A-PHP-PHP-20616/84
Denial of Service	2016-05-21	7.5	Zend/zend_exceptions.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not validate certain Exception objects, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger	https://bugs.php.net/bug.php?id=70121	A-PHP-PHP-20616/85

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

			unintended method execution via crafted serialized data. **Reference : CVE-2015-8876**		
	2016-05-21	5	The openssl_random_pseudo_bytes function in ext/openssl/openssl.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 incorrectly relies on the deprecated RAND_pseudo_bytes function, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors. **Reference : CVE-2015-8867**	http://git.php.net/?p=php-src.git;a=commit;h=16023f3e3b9c06cf677c3c980e8d574e4c162827	A-PHP-PHP-20616/86
	2016-05-21	6.8	ext/libxml/libxml.c in PHP before 5.5.22 and 5.6.x before 5.6.6, when PHP-FPM is used, does not isolate each thread from libxml_disable_entity_loader changes in other threads, which allows remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks via a crafted XML document, a related issue to CVE-2015-5161. **Reference : CVE-2015-8866**	http://git.php.net/?p=php-src.git;a=commit;h=de31324c221c1791b26350ba106cc26bad23ace9	A-PHP-PHP-20616/87
PHP;Xmlsoft					
PHP/Libxml2: *PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language. libxml2 is a software library for parsing XML documents. It is also the basis for the libxslt library which processes XSLT-1.0 stylesheets.*					
Denial of Service	2016-05-16	5	The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility	http://php.net/ChangeLog-5.php	A-PHP-PHP/L-20616/88

			of a NULL valuePop return value before proceeding with a free operation after the principal argument loop, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6837. **Reference : CVE-2015-6838**		
HP;Xmlsoft					
PHP/Libxml2: *PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language. libxml2 is a software library for parsing XML documents. It is also the basis for the libxslt library which processes XSLT-1.0 stylesheets.*					
	2016-05-16	5	The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation during initial error checking, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6838. **Reference : CVE-2015-6837**	http://php.net/ChangeLog-5.php	A-PHP-PHP/L-20616/89
Plupload;Wordpress					
Plupload/Wordpress: *Plupload is JavaScript API for building file uploaders. WordPress is web software you can use to create a beautiful website, blog, or app.*					
XSS	2016-05-21	4.3	Cross-site scripting (XSS) vulnerability in plupload.flash.swf in Plupload before 2.1.9, as used in WordPress before 4.5.2, allows remote	https://wordpress.org/news/2016/05/wordpress-4-5-2/	A-PLU-PLUPL-20616/90

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

			attackers to inject arbitrary web script or HTML via a Same-Origin Method Execution (SOME) attack. **Reference : CVE-2016-4566**		
Pulsesecure					
Pulse Connect Secure: *Pulse Connect Secure is 15 years of innovation and refinement which has led to the most reliable and feature rich VPN built for the next generation.*					
	2016-05-26	5	Pulse Connect Secure (PCS) 8.2 before 8.2r1 allows remote attackers to disclose sign in pages via unspecified vectors. **Reference : CVE-2016-4792**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40212	A-PUL-PULSE-20616/91
	2016-05-26	6.4	The administrative user interface in Pulse Connect Secure (PCS) 8.2 before 8.2r1, 8.1 before 8.1r2, 8.0 before 8.0r9, and 7.4 before 7.4r13.4 allows remote administrators to enumerate files, read arbitrary files, and conduct server side request forgery (SSRF) attacks via unspecified vectors. **Reference : CVE-2016-4791**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40210	A-PUL-PULSE-20616/92
XSS	2016-05-26	3.5	Cross-site scripting (XSS) vulnerability in the administrative user interface in Pulse Connect Secure (PCS) 8.2 before 8.2r1, 8.1 before 8.1r2, 8.0 before 8.0r9, and 7.4 before 7.4r13.4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference : CVE-2016-4790**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40211	A-PUL-PULSE-20616/93
XSS	2016-05-26	4.3	Cross-site scripting (XSS) vulnerability in the system configuration section in the administrative user interface in Pulse Connect Secure (PCS) 8.2 before 8.2r1, 8.1 before 8.1r2, 8.0	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40209	A-PUL-PULSE-20616/94

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

			before 8.0r9, and 7.4 before 7.4r13.4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference : CVE-2016-4789**		
	2016-05-26	5	Pulse Connect Secure (PCS) 8.2 before 8.2r1, 8.1 before 8.1r2, 8.0 before 8.0r10, and 7.4 before 7.4r13.4 allow remote attackers to read an unspecified system file via unknown vectors. **Reference : CVE-2016-4788**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40208	A-PUL-PULSE-20616/95
	2016-05-26	6.4	Pulse Connect Secure (PCS) 8.2 before 8.2r1, 8.1 before 8.1r2, 8.0 before 8.0r10, and 7.4 before 7.4r13.4 allow remote attackers to read sensitive system authentication files in an unspecified directory via unknown vectors. **Reference : CVE-2016-4787**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40207	A-PUL-PULSE-20616/96
Denial of Service	2016-05-26	7.8	Pulse Connect Secure (PCS) 8.2 before 8.2r1, 8.1 before 8.1r3, 8.0 before 8.0r11, and 7.4 before 7.4r13.4 allow remote attackers to cause a denial of service (CPU consumption) via unspecified vectors. **Reference : CVE-2016-4786**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40206	A-PUL-PULSE-20616/97
Qemu					
Qemu: *QEMU (short for Quick Emulator) is a free and open-source hosted hypervisor that performs hardware virtualization. QEMU is a hosted virtual machine monitor*					
Denial of Service Overflow	2016-05-20	2.1	The get_cmd function in hw/scsi/esp.c in the 53C9X Fast SCSI Controller (FSC) support in QEMU does not properly check DMA length, which allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) via	https://bugzilla.redhat.com/show_bug.cgi?id=1337505	A-QEM-QEMU-20616/98

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

			unspecified vectors, involving an SCSI command. **Reference : CVE-2016-4441**		
Denial of Service Exec Code Overflow	2016-05-20	4.6	The esp_reg_write function in hw/scsi/esp.c in the 53C9X Fast SCSI Controller (FSC) support in QEMU does not properly check command buffer length, which allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) or potentially execute arbitrary code on the QEMU host via unspecified vectors. **Reference : CVE-2016-4439**	https://bugzilla.redhat.com/show_bug.cgi?id=1337502	A-QEM-QEMU-20616/99
Denial of Service	2016-05-23	4.9	The ehci_process_itd function in hw/usb/hcd-ehci.c in QEMU allows local guest OS administrators to cause a denial of service (infinite loop and CPU consumption) via a circular isochronous transfer descriptor (iTD) list. **Reference : CVE-2015-8558**	https://bugzilla.redhat.com/show_bug.cgi?id=1277983	A-QEM-QEMU-20616/100
Gain Info	2016-05-25	2.1	The patch_instruction function in hw/i386/kvmvapic.c in QEMU does not initialize the imm32 variable, which allows local guest OS administrators to obtain sensitive information from host stack memory by accessing the Task Priority Register (TPR). **Reference : CVE-2016-4020**	https://bugzilla.redhat.com/show_bug.cgi?id=1313686	A-QEM-QEMU-20616/101
Rubygems					
Safemode: *Safe mode is a troubleshooting option for Windows that starts your computer in a limited state.*					
Gain Info	2016-	6.8	The Safemode gem before	https://github	A-RUB-

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

	05-20		1.2.4 for Ruby, when initialized with a delegate object that is a Rails controller, allows context-dependent attackers to obtain sensitive information via the inspect method. **Reference : CVE-2016-3693**	.com/svenfuchs/safemode/commit/0f764a1720a3a68fd2842e21377c8bfad6d7126f	SAFEM-20616/102
Symantec					
Anti-virus Engine: *At the heart of any antivirus program lies its engine – that is, the module responsible for scanning objects and detecting malicious programs.*					
Denial of Service Exec Code	2016-05-19	9.4	The kernel component in Symantec Anti-Virus Engine (AVE) 20151.1 before 20151.1.1.4 allows remote attackers to execute arbitrary code or cause a denial of service (memory access violation and system crash) via a malformed PE header file. **Reference : CVE-2016-2208**	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&suid=20160516_00	A-SYM-ANTI--20616/103
Theforeman					
Foreman: *Foreman is an open source complete life cycle systems management tool for provisioning, configuring and monitoring of physical and virtual servers.*					
Exec Code	2016-05-20	6.8	Eval injection vulnerability in tftp_api.rb in the TFTP module in the Smart-Proxy in Foreman before 1.10.4 and 1.11.x before 1.11.2 allows remote attackers to execute arbitrary code via the PXE template type portion of the PATH_INFO to tftp/. **Reference : CVE-2016-3728**	http://projects.theforeman.org/issues/14931	A-THE-FOREM-20616/104
NA	2016-05-20	6.5	Foreman before 1.10.3 and 1.11.0 before 1.11.0-RC2 allow remote authenticated users to read, modify, or delete private bookmarks	http://theforeman.org/security.html#2016-2100	A-THE-FOREM-20616/105

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

			by leveraging the (1) edit_bookmarks or (2) destroy_bookmarks permission. **Reference : CVE-2016-2100**		
Trend Micro					
Mobile Security: *Trend Micro Mobile Security provides comprehensive protection that includes antivirus and performance-boosting tools for Android devices.*					
Gain Info	2016-05-23	5.8	Trend Micro Mobile Security for iOS before 3.2.1188 does not verify the X.509 certificate of the mobile application login server, which allows man-in-the-middle attackers to spoof this server and obtain sensitive information via a crafted certificate. **Reference : CVE-2016-3664**	https://esupport.trendmicro.com/en-us/home/pages/technical-support/1114151.aspx	A-TRE-MOBIL-20616/106
Vmware					
Player;Workstation: *VMware Workstation Player is the best way to deliver virtual machines and multiple operating systems*					
Gain Privileges	2016-05-18	10	VMware Workstation 11.x before 11.1.3 and VMware Player 7.x before 7.1.3 on Windows incorrectly access an executable file, which allows host OS users to gain host OS privileges via unspecified vectors. **Reference : CVE-2016-2077**	http://www.vmware.com/security/advisories/VMSA-2016-0005.html	A-VMW-PLAYE-20616/107
Wordpress					
Wordpress: *WordPress is web software you can use to create a beautiful website, blog, or app.*					
NA	2016-05-21	5	The wp_http_validate_url function in wp-includes/http.php in WordPress before 4.4.2 allows remote attackers to conduct server-side request forgery (SSRF) attacks via a zero value in the first octet of an IPv4 address. **Reference : CVE-2016-2222**	https://wordpress.org/news/2016/02/wordpress-4-4-2-security-and-maintenance-release/	A-WOR-WORDP-20616/108
	2016-	5.8	Open redirect vulnerability	https://wordp	A-WOR-

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

	05-21		in the wp_validate_redirect function in wp-includes/pluggable.php in WordPress before 4.4.2 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a malformed URL that triggers incorrect hostname parsing, as demonstrated by an https:example.com URL. **Reference : CVE-2016-2221**	ress.org/news/2016/02/wordpress-4-4-2-security-and-maintenance-release/	WORDP-20616/109
XSS	2016-05-21	4.3	Multiple cross-site scripting (XSS) vulnerabilities in wp-includes/class-wp-theme.php in WordPress before 4.4.1 allow remote attackers to inject arbitrary web script or HTML via a (1) stylesheet name or (2) template name to wp-admin/customize.php. **Reference : CVE-2016-1564**	https://core.trac.wordpress.org/changeset/36185	A-WOR-WORDP-20616/110
XSS	2016-05-21	4.3	Cross-site scripting (XSS) vulnerability in wp-includes/wp-db.php in WordPress before 4.2.2 allows remote attackers to inject arbitrary web script or HTML via a long comment that is improperly stored because of limitations on the MySQL TEXT data type. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-3440. **Reference : CVE-2015-8834**	https://wordpress.org/news/2015/05/wordpress-4-2-2/	A-WOR-WORDP-20616/111
XSS	2016-05-21	3.5	Cross-site scripting (XSS) vulnerability in the user list table in WordPress before 4.3.1 allows remote authenticated users to	https://security-tracker.debian.org/tracker/CVE-2015-	A-WOR-WORDP-20616/112

			inject arbitrary web script or HTML via a crafted e-mail address, a different vulnerability than CVE-2015-5714. **Reference : CVE-2015-7989**	7989	
Bypass	2016-05-21	4	The mw_editPost function in wp-includes/class-wp-xmlrpc-server.php in the XMLRPC subsystem in WordPress before 4.3.1 allows remote authenticated users to bypass intended access restrictions, and arrange for a private post to be published and sticky, via unspecified vectors. **Reference : CVE-2015-5715**	https://security-tracker.debian.org/tracker/CVE-2015-5715	A-WOR-WORDP-20616/113
XSS	2016-05-21	4.3	Cross-site scripting (XSS) vulnerability in WordPress before 4.3.1 allows remote attackers to inject arbitrary web script or HTML by leveraging the mishandling of unclosed HTML elements during processing of shortcode tags. **Reference : CVE-2015-5714**	https://wordpress.org/news/2015/09/wordpress-4-3-1/	A-WOR-WORDP-20616/114
Huawei/Huawei					
ATH;Cherryplus/Ath Firmware;Cherryplus Firmware;Plk Firmware;Rio Firmware: *The latest addition to the critically acclaimed M-Series line, the ATH-M70x professional studio monitor headphones feature proprietary 45 mm large-aperture drivers and are tuned to accurately reproduce extreme low and high frequencies (5 to 40,000 Hz) while maintaining perfect balance; CherryPlus is the Mobile Dialer that allows to make VoIP calls from any of the android devices and it uses 3G/Edge/Wi-Fi Internet connectivity.*					
XSS	2016-05-25	4.3	Cross-site scripting (XSS) vulnerability in the email APP in Huawei PLK smartphones with software AL10C00 before AL10C00B211 and AL10C92 before AL10C92B211; ATH smartphones with software AL00C00 before AL00C00B361, CL00C92	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160507-01-emailapp-en	H-HUA-ATH;C-20616/115

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

			before CL00C92B361, TL00HC01 before TL00HC01B361, and UL00C00 before UL00C00B361; CherryPlus smartphones with software TL00C00 before TL00C00B553, UL00C00 before UL00C00B553, and TL00MC01 before TL00MC01B553; and RIO smartphones with software AL00C00 before AL00C00B360 allows remote attackers to inject arbitrary web script or HTML via an email message. **Reference : CVE-2016-4575**		
Operating System					
Apple					
Apple Tv;Iphone Os;Mac Os X: *Apple TV is a digital media player and a microconsole developed and sold by Apple Inc. iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware. OS X is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc.*					
Denial of Service	2016-05-20	4.3	IOAcceleratorFamily in Apple iOS before 9.3.2, OS X before 10.11.5, and tvOS before 9.2.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted app. **Reference : CVE-2016-1814**	https://support.apple.com/HT206564	O-APP-APPLE-20616/116
Gain Info	2016-05-20	5	The CFNetwork Proxies subsystem in Apple iOS before 9.3.2, OS X before 10.11.5, and tvOS before 9.2.1 mishandles URLs in http and https requests, which allows remote attackers to obtain sensitive information via unspecified vectors. **Reference : CVE-2016-1801**	https://support.apple.com/HT206568	O-APP-APPLE-20616/117

Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	OpenGL, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. **Reference : CVE-2016-1847**	https://support.apple.com/HT206568	O-APP-APPLE-20616/118
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	libxslt, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. **Reference : CVE-2016-1841**	https://support.apple.com/HT206568	O-APP-APPLE-20616/119
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, and CVE-2016-1839. **Reference : CVE-2016-1840**	https://support.apple.com/HT206568	O-APP-APPLE-20616/120
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different	https://support.apple.com/HT206568	O-APP-APPLE-20616/121

			vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, and CVE-2016-1840. **Reference : CVE-2016-1839**		
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1836, CVE-2016-1837, CVE-2016-1839, and CVE-2016-1840. **Reference : CVE-2016-1838**	https://support.apple.com/HT206568	O-APP-APPLE-20616/122
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1836, CVE-2016-1838, CVE-2016-1839, and CVE-2016-1840. **Reference : CVE-2016-1837**	https://support.apple.com/HT206568	O-APP-APPLE-20616/123
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted	https://support.apple.com/HT206568	O-APP-APPLE-20616/124

			XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, and CVE-2016-1840. **Reference : CVE-2016-1836**		
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, and CVE-2016-1840. **Reference : CVE-2016-1834**	https://support.apple.com/HT206568	O-APP-APPLE-20616/125
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1834, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, and CVE-2016-1840. **Reference : CVE-2016-1833**	https://support.apple.com/HT206568	O-APP-APPLE-20616/126
Denial of Service Overflow +Priv Mem. Corr.	2016-05-20	4.6	libc in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified	https://support.apple.com/HT206568	O-APP-APPLE-20616/127

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

			vectors. **Reference : CVE-2016-1832**		
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	The kernel in Apple iOS before 9.3.2 and OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference : CVE-2016-1831**	https://support.apple.com/HT206568	O-APP-APPLE-20616/128
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	8.5	The kernel in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1827, CVE-2016-1828, and CVE-2016-1829. **Reference : CVE-2016-1830**	https://support.apple.com/HT206568	O-APP-APPLE-20616/129
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	The kernel in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1827, CVE-2016-1828, and CVE-2016-1830. **Reference : CVE-2016-1829**	https://support.apple.com/HT206568	O-APP-APPLE-20616/130
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	The kernel in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a	https://support.apple.com/HT206568	O-APP-APPLE-20616/131

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

			privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1827, CVE-2016-1829, and CVE-2016-1830. **Reference : CVE-2016-1828**		
OS Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	The kernel in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1828, CVE-2016-1829, and CVE-2016-1830. **Reference : CVE-2016-1827**	https://support.apple.com/HT206568	O-APP-APPLE-20616/132
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	IOHIDFamily in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1823. **Reference : CVE-2016-1824**	https://support.apple.com/HT206568	O-APP-APPLE-20616/133
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	IOHIDFamily in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1824.	https://support.apple.com/HT206568	O-APP-APPLE-20616/134

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

			Reference : CVE-2016-1823		
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	IOAcceleratorFamily in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1817 and CVE-2016-1818. **Reference : CVE-2016-1819**	https://support.apple.com/HT206568	O-APP-APPLE-20616/135
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	IOAcceleratorFamily in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1817 and CVE-2016-1819. **Reference : CVE-2016-1818**	https://support.apple.com/HT206568	O-APP-APPLE-20616/136
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	IOAcceleratorFamily in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1818 and CVE-2016-1819. **Reference : CVE-2016-1817**	https://support.apple.com/HT206568	O-APP-APPLE-20616/137

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

Denial of Service Exec Code	2016-05-20	9.3	IOAcceleratorFamily in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app. **Reference : CVE-2016-1813**	https://support.apple.com/HT206568	O-APP-APPLE-20616/138
Denial of Service	2016-05-20	5	ImageIO in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted image. **Reference : CVE-2016-1811**	https://support.apple.com/HT206568	O-APP-APPLE-20616/139
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	The Disk Images subsystem in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference : CVE-2016-1808**	https://support.apple.com/HT206568	O-APP-APPLE-20616/140
Gain Info	2016-05-20	2.6	Race condition in the Disk Images subsystem in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 allows local users to obtain sensitive information from kernel memory via unspecified vectors. **Reference : CVE-2016-1807**	https://support.apple.com/HT206568	O-APP-APPLE-20616/141
Denial of Service Exec Code	2016-05-20	9.3	CoreCapture in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1,	https://support.apple.com/HT206568	O-APP-APPLE-20616/14

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

			and watchOS before 2.2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app. **Reference : CVE-2016-1803**		2
Gain Info	2016-05-20	4.3	CCCrypt in CommonCrypto in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1 mishandles return values during key-length calculations, which allows attackers to obtain sensitive information via a crafted app. **Reference : CVE-2016-1802**	https://support.apple.com/HT206568	O-APP-APPLE-20616/143
Iphone Os: *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.*					
Gain Info	2016-05-20	2.1	Siri in Apple iOS before 9.3.2 does not block data detectors within results in the lock-screen state, which allows physically proximate attackers to obtain sensitive contact and photo information via unspecified vectors. **Reference : CVE-2016-1852**	https://support.apple.com/HT206568	O-APP-IPHON-20616/144
Overflow Gain Info	2016-05-20	4.3	Buffer overflow in the Accessibility component in Apple iOS before 9.3.2 allows attackers to obtain sensitive kernel memory-layout information via a crafted app. **Reference : CVE-2016-1790**	https://support.apple.com/HT206568	O-APP-IPHON-20616/145
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	libxml2, as used in Apple iOS before 9.3.2 and OS X before 10.11.5, allows remote attackers to execute arbitrary code or cause a	https://support.apple.com/HT206568	O-APP-IPHON-20616/146

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

			denial of service (memory corruption) via a crafted XML document. **Reference : CVE-2016-1835**		
Gain Info	2016-05-20	5	MapKit in Apple iOS before 9.3.2, OS X before 10.11.5, and watchOS before 2.2.1 does not use HTTPS for shared links, which allows remote attackers to obtain sensitive information by sniffing the network for HTTP traffic. **Reference : CVE-2016-1842**	https://support.apple.com/HT206566	O-APP-IPHON-20616/147
Mac Os X: *OS X (originally Mac OS X) is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc. It is designed to run on Macintosh computers, having been pre-installed on all Macs since 2002.*					
Gain Info	2016-05-20	5	Tcl in Apple OS X before 10.11.5 allows remote attackers to obtain sensitive information by leveraging SSLv2 support. **Reference : CVE-2016-1853**	https://support.apple.com/HT206567	O-APP-MAC O-20616/148
	2016-05-20	2.1	The Screen Lock feature in Apple OS X before 10.11.5 mishandles password profiles, which allows physically proximate attackers to reset expired passwords in the lock-screen state via unspecified vectors. **Reference : CVE-2016-1851**	https://support.apple.com/HT206567	O-APP-MAC O-20616/149
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	SceneKit in Apple OS X before 10.11.5 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted file. **Reference : CVE-2016-1850**	https://support.apple.com/HT206567	O-APP-MAC O-20616/150
Denial of Service Exec Code Overflow	2016-05-20	6.8	QuickTime in Apple OS X before 10.11.5 allows remote attackers to execute arbitrary code or cause a	https://support.apple.com/HT206567	O-APP-MAC O-20616/151

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

Mem. Corr.			denial of service (memory corruption) via a crafted file. **Reference : CVE-2016-1848**		
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	The NVIDIA Graphics Drivers subsystem in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference : CVE-2016-1846**	https://support.apple.com/HT206567	O-APP-MAC O-20616/152
	2016-05-20	5	The Messages component in Apple OS X before 10.11.5 mishandles roster changes, which allows remote attackers to modify contact lists via unspecified vectors. **Reference : CVE-2016-1844**	https://support.apple.com/HT206567	O-APP-MAC O-20616/153
Gain Info	2016-05-20	5	The Messages component in Apple OS X before 10.11.5 mishandles filename encoding, which allows remote attackers to obtain sensitive information via unspecified vectors. **Reference : CVE-2016-1843**	https://support.apple.com/HT206567	O-APP-MAC O-20616/154
Exec Code Overflow	2016-05-20	9.3	Integer overflow in the dtrace implementation in the kernel in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context via a crafted app. **Reference : CVE-2016-1826**	https://support.apple.com/HT206567	O-APP-MAC O-20616/155
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	IOHIDFamily in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause	https://support.apple.com/HT206567	O-APP-MAC O-20616/156

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

			a denial of service (memory corruption) via a crafted app. **Reference : CVE-2016-1825**		
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	IOFireWireFamily in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference : CVE-2016-1822**	https://support.apple.com/HT206567	O-APP-MAC O-20616/157
Denial of Service Exec Code	2016-05-20	9.3	IOAudioFamily in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app. **Reference : CVE-2016-1821**	https://support.apple.com/HT206567	O-APP-MAC O-20616/158
Exec Code Overflow	2016-05-20	9.3	Buffer overflow in IOAudioFamily in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context via a crafted app. **Reference : CVE-2016-1820**	https://support.apple.com/HT206567	O-APP-MAC O-20616/159
Denial of Service Exec Code	2016-05-20	9.3	IOAcceleratorFamily in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app. **Reference : CVE-2016-1816**	https://support.apple.com/HT206567	O-APP-MAC O-20616/160
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	IOAcceleratorFamily in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause	https://support.apple.com/HT206567	O-APP-MAC O-20616/161

			a denial of service (memory corruption) via a crafted app. **Reference : CVE-2016-1815**		
Exec Code Overflow	2016-05-20	9.3	Buffer overflow in Intel Graphics Driver in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context via a crafted app. **Reference : CVE-2016-1812**	https://support.apple.com/HT206567	O-APP-MAC O-20616/162
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	The Graphics Drivers subsystem in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference : CVE-2016-1810**	https://support.apple.com/HT206567	O-APP-MAC O-20616/163
	2016-05-20	7.8	Disk Utility in Apple OS X before 10.11.5 uses incorrect encryption keys for disk images, which has unspecified impact and attack vectors. **Reference : CVE-2016-1809**	https://support.apple.com/HT206567	O-APP-MAC O-20616/164
Exec Code	2016-05-20	9.3	Crash Reporter in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context via a crafted app. **Reference : CVE-2016-1806**	https://support.apple.com/HT206567	O-APP-MAC O-20616/165
Exec Code	2016-05-20	9.3	CoreStorage in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context via a crafted app. **Reference : CVE-2016-1805**	https://support.apple.com/HT206567	O-APP-MAC O-20616/166
Denial of	2016-	9.3	The Multi-Touch subsystem	https://suppo	O-APP-

Service Exec Code Overflow Mem. Corr.	05-20		in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference : CVE-2016-1804**	rt.apple.com/HT206567	MAC O-20616/167
Exec Code	2016-05-20	9.3	Captive Network Assistant in Apple OS X before 10.11.5 mishandles a custom URL scheme, which allows user-assisted remote attackers to execute arbitrary code via unspecified vectors. **Reference : CVE-2016-1800**	https://support.apple.com/HT206567	O-APP-MAC O-20616/168
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	Audio in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference : CVE-2016-1799**	https://support.apple.com/HT206567	O-APP-MAC O-20616/169
Denial of Service	2016-05-20	4.3	Audio in Apple OS X before 10.11.5 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted app. **Reference : CVE-2016-1798**	https://support.apple.com/HT206567	O-APP-MAC O-20616/170
Exec Code Bypass	2016-05-20	9.3	Apple Type Services (ATS) in Apple OS X before 10.11.5 allows attackers to bypass intended FontValidator sandbox-policy restrictions and execute arbitrary code in a privileged context via a crafted app. **Reference : CVE-2016-1797**	https://support.apple.com/HT206567	O-APP-MAC O-20616/171
Denial of Service Gain Info	2016-05-20	4.3	Apple Type Services (ATS) in Apple OS X before 10.11.5 allows attackers to obtain sensitive kernel memory-layout information or cause	https://support.apple.com/HT206567	O-APP-MAC O-20616/172

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

			a denial of service (out-of-bounds memory access) via a crafted app. **Reference : CVE-2016-1796**		
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	AppleGraphicsPowerManagement in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference : CVE-2016-1795**	https://support.apple.com/HT206567	O-APP-MAC O-20616/173
Denial of Service Exec Code	2016-05-20	9.3	AppleGraphicsControl in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app, a different vulnerability than CVE-2016-1793. **Reference : CVE-2016-1794**	https://support.apple.com/HT206567	O-APP-MAC O-20616/174
Denial of Service Exec Code	2016-05-20	9.3	AppleGraphicsControl in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app, a different vulnerability than CVE-2016-1794. **Reference : CVE-2016-1793**	https://support.apple.com/HT206567	O-APP-MAC O-20616/175
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	9.3	The AMD subsystem in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference : CVE-2016-1792**	https://support.apple.com/HT206567	O-APP-MAC O-20616/176
Gain Info	2016-	4.3	The AMD subsystem in	https://suppo	O-APP-

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

	05-20		Apple OS X before 10.11.5 allows attackers to obtain sensitive kernel memory-layout information via a crafted app. **Reference : CVE-2016-1791**	rt.apple.com/HT206567	MAC O-20616/177
Ios Xr: *IOS XR is a train of Cisco Systems' widely deployed Internetworking Operating System (IOS), used on their high-end carrier-grade routers such as the CRS series, 12000 series, and ASR9000 series.*					
Denial of Service	2016-05-24	5	Cisco IOS XR through 5.3.2 mishandles Local Packet Transport Services (LPTS) mishandles flow-base entries, which allows remote attackers to cause a denial of service (session drop) by making many connection attempts to open TCP ports, aka Bug ID CSCux95576. **Reference : CVE-2016-1407**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160519-ios-xr	O-CIS-IOS X-20616/178
Fortinet					
Fortisandbox Firmware: *FortiSandbox is an Advanced Threat Protection Appliance designed to identify the highly targeted and tailored attacks that increasingly bypass traditional defenses and lurk within networks.*					
XSS	2016-05-26	4.3	Multiple cross-site scripting (XSS) vulnerabilities in the Web User Interface (WebUI) in Fortinet FortiSandbox before 2.1 allow remote attackers to inject arbitrary web script or HTML via the (1) serial parameter to alerts/summary/profile/; the (2) urlForCreatingReport parameter to csearch/report/export/; the (3) id parameter to analysis/detail/download/screenshot; or vectors related to (4) "Fortiview threats by users search filtered by vdom" or (5) "PCAP file download generated by the VM scan feature." **Reference : CVE-2015-7360**	http://fortiguard.com/advisory/multiple-XSS-vulnerabilities-in-fortisandbox-webui	O-FOR-FORTI-20616/179

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

Freebsd					
Freebsd: *FreeBSD is an operating system for a variety of platforms which focuses on features, speed, and stability.*					
Denial of Service Overflow Gain Privileges	2016-05-25	7.2	Integer signedness error in the sockargs function in sys/kern/uipc_syscalls.c in FreeBSD 10.1 before p34, 10.2 before p17, and 10.3 before p3 allows local users to cause a denial of service (memory overwrite and kernel panic) or gain privileges via a negative buflen argument, which triggers a heap-based buffer overflow. **Reference : CVE-2016-1887**		O-FRE-FREEB-20616/180
Denial of Service Overflow Gain Priv Gain Info	2016-05-25	7.2	Integer signedness error in the genkbd_commonioctl function in sys/dev/kbd/kbd.c in FreeBSD 9.3 before p42, 10.1 before p34, 10.2 before p17, and 10.3 before p3 allows local users to obtain sensitive information from kernel memory, cause a denial of service (memory overwrite and kernel crash), or gain privileges via a negative value in the flen structure member in the arg argument in a SETFKEY ioctl call, which triggers a "two way heap and stack overflow." **Reference : CVE-2016-1886**	https://security.FreeBSD.org/patches/SA-16:18/atkbd.patch	O-FRE-FREEB-20616/181
Huawei					
Ips Module Firmware;Ngfw Module Firmware;Nip6300 Firmware;Nip6600 Firmware;Secospace AntidDenial of Service8000 Firmware;Secospace Usg6300 Firmware;Secospace Usg6500 Firmware;Secospace Usg6600 Firmware;Usg9500 Firmware: *The IPS module runs advanced IPS software that provides proactive, full-featured intrusion prevention services to stop malicious traffic,*					

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

including worms and network viruses, before they can affect your network. Next-Generation Firewalls (NGFW) with Layer 8 Identity-based technology offer actionable intelligence and controls to enterprises that allow complete security controls over L2-L8 for their future-ready security. HUAWEI NIP6300/6600 series is an advanced, new generation intrusion prevention system (NGIPS) designed to provide application and service security; Huawei Anti-DDenial of Service8000 DDenial of Service Protection Systems provides fast, Terabit-per-second protection to defend infrastructure, applications, and data.					
Denial of Service Exec Code Overflow	2016-05-23	7.5	Buffer overflow in the Application Specific Packet Filtering (ASPF) functionality in the Huawei IPS Module, NGFW Module, NIP6300, NIP6600, Secospace USG6300, USG6500, USG6600, USG9500, and AntiDDenial of Service8000 devices with software before V500R001C20SPC100 allows remote attackers to cause a denial of service or execute arbitrary code via a crafted packet, related to "illegitimate parameters." **Reference : CVE-2016-4576**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160511-01-aspf-en	O-HUA-IPS M-20616/182
Mate 8 Firmware: *Huawei Mate 8 is a very stylish smartphone from Huawei with large 6 inch display and Kirin 950 CPU.*					
Denial of Service Overflow Gain Privileges	2016-05-26	9.3	Buffer overflow in the Wi-Fi driver in Huawei Mate 8 NXT-AL before NXT-AL10C00B182, NXT-CL before NXT-CL00C92B182, NXT-DL before NXT-DL00C17B182, and NXT-TL before NXT-TL00C01B182 allows attackers to cause a denial of service (crash) or possibly gain privileges via a crafted application, aka HWPSIRT-2016-03021. **Reference : CVE-2016-3681**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160520-02-smartphone-en	O-HUA-MATE-20616/183
Denial of Service Overflow Gain Priv	2016-05-26	9.3	Buffer overflow in the Wi-Fi driver in Huawei Mate 8 NXT-AL before NXT-AL10C00B182, NXT-CL before NXT-CL00C92B182, NXT-DL before NXT-	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-	O-HUA-MATE-20616/184

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

			DL00C17B182, and NXT-TL before NXT-TL00C01B182 allows attackers to cause a denial of service (crash) or possibly gain privileges via a crafted application, aka HWPSIRT-2016-03020. **Reference : CVE-2016-3680**	20160520-02-smartphone-en	
Ngfw Module Firmware;Secospace Usg6300 Firmware;Secospace Usg6500 Firmware;Secospace Usg6600 Firmware;Usg9500 Firmware: *Next-Generation Firewalls (NGFW) with Layer 8 Identity-based technology offer actionable intelligence and controls to enterprises that allow complete security controls over L2-L8 for their future-ready security. HUAWEI NIP6300/6600 series is an advanced, new generation intrusion prevention system (NGIPS) designed to provide application and service security; Huawei Anti-DDenial of Service8000 DDenial of Service Protection Systems provides fast, Terabit-per-second protection to defend infrastructure, applications, and data.*					
Denial of Service Exec Code Overflow	2016-05-23	6.8	Buffer overflow in the Smart DNS functionality in the Huawei NGFW Module and Secospace USG6300, USG6500, USG6600, and USG9500 firewalls with software before V500R001C20SPC100 allows remote attackers to cause a denial of service or execute arbitrary code via a crafted packet, related to "illegitimate parameters." **Reference : CVE-2016-4577**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160511-01-dns-en	O-HUA-NGFW-20616/185
Denial of Service Exec Code	2016-05-23	5.1	Huawei S12700 switches with software before V200R008C00SPC500 and S5700 switches with software before V200R005SPH010, when the debug switch is enabled, allows remote attackers to cause a denial of service or execute arbitrary code via crafted DNS packets. **Reference : CVE-2016-4087**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160427-01-dns-en	O-HUA-S1270-20616/186
Linux					
Linux Kernel: *The Linux kernel is a Unix-like computer operating system kernel.*					
Denial of	2016-	7.2	The tipc_nl_publ_dump	https://github	O-LIN-

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

Service	05-23		function in net/tipc/socket.c in the Linux kernel through 4.6 does not verify socket existence, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a dumpit operation. **Reference : CVE-2016-4951**	.com/torvalds/linux/commit/45e093ae2830cd1264677d47ff9a95a71f5d9f9c	LINUX-20616/187
Gain Info	2016-05-23	7.2	The get_rock_ridge_filename function in fs/isofs/rock.c in the Linux kernel before 4.5.5 mishandles NM (aka alternate name) entries containing \0 characters, which allows local users to obtain sensitive information from kernel memory or possibly have unspecified other impact via a crafted isofs filesystem. **Reference : CVE-2016-4913**	https://github.com/torvalds/linux/commit/99d825822eade8d827a1817357cbf3f889a552d6	O-LIN-LINUX-20616/188
Denial of Service Mem. Corr.	2016-05-23	7.2	Use-after-free vulnerability in drivers/net/ppp/ppp_generic.c in the Linux kernel before 4.5.2 allows local users to cause a denial of service (memory corruption and system crash, or spinlock) or possibly have unspecified other impact by removing a network namespace, related to the ppp_register_net_channel and ppp_unregister_channel functions. **Reference : CVE-2016-4805**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=1f461dcdd296eecedaffffc6bae2bfa90bd7eb89	O-LIN-LINUX-20616/189
Denial of Service	2016-05-23	7.2	Use-after-free vulnerability in mm/percpu.c in the Linux kernel through 4.6 allows local users to cause a	https://bugzilla.redhat.com/show_bug.cgi?	O-LIN-LINUX-20616/190

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

			denial of service (BUG) or possibly have unspecified other impact via crafted use of the mmap and bpf system calls. **Reference : CVE-2016-4794**	id=1335889	
Denial of Service	2016-05-23	4.9	fs/pnode.c in the Linux kernel before 4.5.4 does not properly traverse a mount propagation tree in a certain case involving a slave mount, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted series of mount system calls. **Reference : CVE-2016-4581**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=5ec0811d30378ae104f250bfc9b3640242d81e3f	O-LIN-LINUX-20616/191
Gain Info	2016-05-23	5	The x25_negotiate_facilities function in net/x25/x25_facilities.c in the Linux kernel before 4.5.5 does not properly initialize a certain data structure, which allows attackers to obtain sensitive information from kernel stack memory via an X.25 Call Request. **Reference : CVE-2016-4580**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=79e48650320e6fba48369fccf13fd045315b19b8	O-LIN-LINUX-20616/192
Gain Info	2016-05-23	2.1	sound/core/timer.c in the Linux kernel through 4.6 does not initialize certain r1 data structures, which allows local users to obtain sensitive information from kernel stack memory via crafted use of the ALSA timer interface, related to the (1) snd_timer_user_ccallback and (2) snd_timer_user_tinterrupt functions. **Reference : CVE-2016-4578**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=9a47e9cff994f37f7f0dbd9ae23740d0f64f9fe6	O-LIN-LINUX-20616/193
Gain Info	2016-	2.1	The snd_timer_user_params	https://bugzill	O-LIN-

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

	05-23		function in sound/core/timer.c in the Linux kernel through 4.6 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via crafted use of the ALSA timer interface. **Reference : CVE-2016-4569**	a.redhat.com/show_bug.cgi?id=1334643	LINUX-20616/194
Denial of Service Overflow	2016-05-23	7.2	drivers/media/v4l2-core/videobuf2-v4l2.c in the Linux kernel before 4.5.3 allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a crafted number of planes in a VIDIOC_DQBUF ioctl call. **Reference : CVE-2016-4568**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=2c1f6951a8a82e6de0d82b1158b5e493fc6c54ab	O-LIN-LINUX-20616/195
Denial of Service	2016-05-23	7.2	The InfiniBand (aka IB) stack in the Linux kernel before 4.5.3 incorrectly relies on the write system call, which allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a uAPI interface. **Reference : CVE-2016-4565**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=e6bd18f57aad1a2d1ef40e646d03ed0f2515c9e3	O-LIN-LINUX-20616/196
Denial of Service	2016-05-23	6.9	The BPF subsystem in the Linux kernel before 4.5.5 mishandles reference counts, which allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted application on (1) a system with more than 32 Gb of memory, related to the program reference count or (2) a 1 Tb system, related to the map reference count.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=92117d8443bc5afacc8d5ba82e541946310f106e	O-LIN-LINUX-20616/197

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

			Reference : CVE-2016-4558		
Denial of Service Gain Privileges	2016-05-23	7.2	The replace_map_fd_with_map_ptr function in kernel/bpf/verifier.c in the Linux kernel before 4.5.5 does not properly maintain an fd data structure, which allows local users to gain privileges or cause a denial of service (use-after-free) via crafted BPF instructions that reference an incorrect file descriptor. **Reference : CVE-2016-4557**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=8358b02bf67d3a5d8a825070e1aa73f25fb2e4c7	O-LIN-LINUX-20616/198
Gain Info	2016-05-23	2.1	The rtnl_fill_link_ifmap function in net/core/rtnetlink.c in the Linux kernel before 4.5.5 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory by reading a Netlink message. **Reference : CVE-2016-4486**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=5f8e44741f9f216e33736ea4ec65ca9ac03036e6	O-LIN-LINUX-20616/199
Gain Info	2016-05-23	5	The llc_cmsg_rcv function in net/llc/af_llc.c in the Linux kernel before 4.5.5 does not initialize a certain data structure, which allows attackers to obtain sensitive information from kernel stack memory by reading a message. **Reference : CVE-2016-4485**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=b8670c09f37bdf2847cc44f36511a53afc6161fd	O-LIN-LINUX-20616/200
Gain Info	2016-05-23	2.1	The proc_connectinfo function in drivers/usb/core/devio.c in the Linux kernel through 4.6 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=681fef8380eb818c0b845fca5d2ab1dcbab114ee	O-LIN-LINUX-20616/201

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

			USBDEVFS_CONNECTINFO ioctl call. **Reference : CVE-2016-4482**		
XEN					
XEN: *Xen Project is a hypervisor using a microkernel design, providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently*					
Gain Priv	2016-05-18	7.2	The guest_walk_tables function in arch/x86/mm/guest_walk.c in Xen 4.6.x and earlier does not properly handle the Page Size (PS) page table entry bit at the L4 and L3 page table levels, which might allow local guest OS users to gain privileges via a crafted mapping of memory. **Reference : CVE-2016-4480**	http://xenbits.xen.org/xsa/advisory-176.html	O-XEN-XEN-20616/202
Operating System					
Apple					
Apple Tv;Iphone Os/Safari: *Apple TV is a digital media player and a microconsole developed and sold by Apple Inc; iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware; Safari is a web browser developed by Apple based on the WebKit engine.*					
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	The WebKit Canvas implementation in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. **Reference : CVE-2016-1859**	https://support.apple.com/HT206564	O-APP-APPLE-20616/203
Gain Info	2016-05-20	4.3	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, improperly tracks taint attributes, which allows remote attackers to obtain sensitive information via a crafted web site.	https://support.apple.com/HT206564	O-APP-APPLE-20616/204

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

			Reference : CVE-2016-1858		
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1854, CVE-2016-1855, and CVE-2016-1856. **Reference : CVE-2016-1857**	https://support.apple.com/HT206564	O-APP-APPLE-20616/205
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1854, CVE-2016-1855, and CVE-2016-1857. **Reference : CVE-2016-1856**	https://support.apple.com/HT206564	O-APP-APPLE-20616/206
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1854, CVE-2016-1856, and CVE-2016-1857. **Reference : CVE-2016-1855**	https://support.apple.com/HT206564	O-APP-APPLE-20616/207
Denial of Service Exec Code Overflow Mem. Corr.	2016-05-20	6.8	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a	https://support.apple.com/HT206564	O-APP-APPLE-20616/208

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

			denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1855, CVE-2016-1856, and CVE-2016-1857. **Reference : CVE-2016-1854**		
Gain Info	2016-05-20	2.1	The "Clear History and Website Data" feature in Apple Safari before 9.1.1, as used in iOS before 9.3.2 and other products, mishandles the deletion of browsing history, which might allow local users to obtain sensitive information by leveraging read access to a Safari directory. **Reference : CVE-2016-1849**	https://support.apple.com/HT206565	O-APP-IPHON-20616/209

Apple/PHP

Mac Os X/PHP: *OS X is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc. PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language.*

Denial of Service Exec Code Overflow	2016-05-20	7.5	Multiple integer overflows in the mbfl_strcut function in ext/mbstring/libmbfl/mbfl/mbfilter.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted mb_strcut call. **Reference : CVE-2016-4073**	http://www.php.net/ChangeLog-5.php	O-APP-MAC O-20616/210
Exec Code	2016-05-20	7.5	The Phar extension in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via a crafted filename, as demonstrated by mishandling of \0 characters by the	http://www.php.net/ChangeLog-5.php	O-APP-MAC O-20616/211

			phar_analyze_path function in ext/phar/phar.c. **Reference : CVE-2016-4072**		
Exec Code	2016-05-20	7.5	Format string vulnerability in the php_snmp_error function in ext/snmp/snmp.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via format string specifiers in an SNMP::get call. **Reference : CVE-2016-4071**	http://www.php.net/ChangeLog-7.php	O-APP-MAC O-20616/212
Denial of Service Exec Code Overflow	2016-05-20	7.5	The file_check_mem function in funcs.c in file before 5.23, as used in the Fileinfo component in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5, mishandles continuation-level jumps, which allows context-dependent attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code via a crafted magic file. **Reference : CVE-2015-8865**	http://bugs.gw.com/view.php?id=522	O-APP-MAC O-20616/213
Canonical;Debian/Libexpat					
Ubuntu Linux/Debian Linux/Expat: *Ubuntu is an open source software platform that runs everywhere from the smartphone, the tablet and the PC to the server and the cloud; Debian is an operating system and a distribution of Free Software; In computing, Expat is a stream-oriented XML 1.0 parser library, written in C.*					
Denial of Service Exec Code Overflow	2016-05-26	7.5	Expat allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a malformed input document, which triggers a buffer overflow. **Reference : CVE-2016-0718**	https://bugzilla.redhat.com/show_bug.cgi?id=1296102	O-CAN-UBUNT-20616/214

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

Debian/X-stream

Debian Linux/Xstream: *Debian is an operating system and a distribution of Free Software; XStream is a simple library to serialize objects to XML and back again.*

Gain Info	2016-05-17	5	Multiple XML external entity (XXE) vulnerabilities in the (1) Dom4JDriver, (2) DomDriver, (3) JDomDriver, (4) JDom2Driver, (5) SjsxpDriver, (6) StandardStaxDriver, and (7) WstxDriver drivers in XStream before 1.4.9 allow remote attackers to read arbitrary files via a crafted XML document. **Reference : CVE-2016-3674**	https://github.com/x-stream/xstream/issues/25	O-DEB-DEBIA-20616/215

Fedoraproject/Perl

Fedora/Perl: *Fedora is an operating system based on the Linux kernel; Perl is a family of high-level, general-purpose, interpreted, dynamic programming languages. The languages in this family include Perl 5 and Perl 6. Though Perl is not officially an acronym, there are various backronyms in use, the most well-known being "Practical Extraction and Reporting Language".*

Denial of Service	2016-05-25	5	The (1) S_reghop3, (2) S_reghop4, and (3) S_reghopmaybe3 functions in regexec.c in Perl before 5.24.0 allow context-dependent attackers to cause a denial of service (infinite loop) via crafted utf-8 data, as demonstrated by "a\x80." **Reference : CVE-2015-8853**	https://rt.perl.org/Public/Bug/Display.html?id=123562	O-FED-FEDOR-20616/216

Fedoraproject

Fedora/Pgpdump: *Fedora is an operating system based on the Linux kernel; The PGPdump Interface is a web interface to pgpdump, the PGP packet visualizer by Kazu Yamamoto.*

Denial of Service	2016-05-26	7.8	The read_binary function in buffer.c in pgpdump before 0.30 allows context-dependent attackers to cause a denial of service (infinite loop and CPU consumption) via crafted input, as demonstrated by the \xa3\x03 string. **Reference : CVE-2016-**	https://github.com/kazu-yamamoto/pgpdump/pull/16	O-FED-FEDOR-20616/217

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

			4021		
Fedora/Qemu: *Fedora is an operating system based on the Linux kernel; QEMU (short for Quick Emulator) is a free and open-source hosted hypervisor that performs hardware virtualization. QEMU is a hosted virtual machine monitor.*					
Denial of Service	2016-05-23	4.9	The ehci_advance_state function in hw/usb/hcd-ehci.c in QEMU allows local guest OS administrators to cause a denial of service (infinite loop and CPU consumption) via a circular split isochronous transfer descriptor (siTD) list, a related issue to CVE-2015-8558. **Reference : CVE-2016-4037**	http://git.qemu.org/?p=qemu.git;a=commit;h=1ae3f2f178087711f9591350abad133525ba93f2	O-FED-FEDOR-20616/218
Denial of Service Overflow	2016-05-23	4.3	Buffer overflow in the stellaris_enet_receive function in hw/net/stellaris_enet.c in QEMU, when the Stellaris ethernet controller is configured to accept large packets, allows remote attackers to cause a denial of service (QEMU crash) via a large packet. **Reference : CVE-2016-4001**	http://git.qemu.org/?p=qemu.git;a=commit;h=3a15cc0e1ee7168db0782133d2607a6bfa422d66	O-FED-FEDOR-20616/219
Fedora/Leap/GO: *Fedora is an operating system based on the Linux kernel; LEAP, the Long range Energy Alternatives Planning System, is a widely-used software tool for energy policy analysis and climate change mitigation assessment developed at the Stockholm Environment Institute. Go is an open source programming language created at Google in 2007.*					
Denial of Service	2016-05-23	5	The Verify function in crypto/dsa/dsa.go in Go before 1.5.4 and 1.6.x before 1.6.1 does not properly check parameters passed to the big integer library, which might allow remote attackers to cause a denial of service (infinite loop) via a crafted public key to a program that uses HTTPS client certificates or SSH server libraries. **Reference : CVE-2016-3959**	https://go-review.googlesource.com/#/c/21533/	O-FED-FEDOR-20616/220

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

Novell/Quagga

Leap;Opensuse/Quagga: *LEAP, the Long range Energy Alternatives Planning System, is a widely-used software tool for energy policy analysis and climate change mitigation assessment developed at the Stockholm Environment Institute; openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies/ Quagga is a network routing software suite providing implementations of Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Border Gateway Protocol (BGP) and IS-IS for Unix-like platforms, particularly Linux, Solaris, FreeBSD and NetBSD.*

Denial of Service	2016-05-23	5	The bgp_dump_routes_func function in bgpd/ bgp_dump.c in Quagga does not perform size checks when dumping data, which might allow remote attackers to cause a denial of service (assertion failure and daemon crash) via a large BGP packet. **Reference : CVE-2016-4049**		O-NOV-LEAP;-20616/221

Novell/Xmlsoft

Leap/Libxml2: *LEAP, the Long range Energy Alternatives Planning System, is a widely-used software tool for energy policy analysis and climate change mitigation assessment developed at the Stockholm Environment Institute; libxml2 is a software library for parsing XML documents. It is also the basis for the libxslt library which processes XSLT-1.0 stylesheets.*

Denial of Service	2016-05-17	5	The xmlParserEntityCheck , xmlParseAttValueComplex functions in parser.c in libxml2 2.9.3 do not properly keep track of the recursion depth, which allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a crafted XML document containing a large number of nested entity references. **Reference : CVE-2016-3705**	https://bugzilla.gnome.org/show_bug.cgi?id=765207	O-NOV-LEAP/-20616/222
Denial of Service	2016-05-17	5	The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier, when used in recovery mode, allows context-dependent attackers to cause a denial		O-NOV-LEAP/-20616/223

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

			of service (infinite recursion, stack consumption, and application crash) via a crafted XML document. **Reference : CVE-2016-3627**		

Gnome/Novell

Librsvg/Leap;Opensuse: *librsvg is a free software SVG rendering library written as part of the GNOME project, intended to be lightweight and portable/LEAP, the Long range Energy Alternatives Planning System, is a widely-used software tool for energy policy analysis and climate change mitigation assessment developed at the Stockholm Environment Institute; openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies*

Denial of Service	2016-05-20	5	The _rsvg_css_normalize_font_size function in librsvg 2.40.2 allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via circular definitions in an SVG document. **Reference : CVE-2016-4348**	https://git.gnome.org/browse/librsvg/commit/?id=d1c9191949747f6dcfd207831d15dd4ba00e31f2	O-GNO-LIBRS-20616/224

IBM

JavaSdk/Manager;ManagerProxy;Openstack/Desktop Supplementary; Enterprise Linux Desktop Supplementary;Enterprise Linux Hpc Node Supplementary;Enterprise Linux Server Supplementary;Enterprise Linux Server Supplementary Eus; Enterprise Linux Workstation Supplementary;Supplementary/Linux Enterprise Server;Linux Enterprise Software Development Kit: *NA*

Exec Code Overflow	2016-05-24	6.8	Buffer overflow in the Java Virtual Machine (JVM) in IBM SDK, Java Technology Edition 6 before SR16 FP25 (6.0.16.25), 6 R1 before SR8 FP25 (6.1.8.25), 7 before SR9 FP40 (7.0.9.40), 7 R1 before SR3 FP40 (7.1.3.40), and 8 before SR3 (8.0.3.0) allows remote attackers to execute arbitrary code via unspecified vectors. **Reference : CVE-2016-0264**	http://www-01.ibm.com/support/docview.wss?uid=swg21980826	O-IBM-JAVA-20616/225

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


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