Vulnerability Type(s)	Publish Date	CVSS	Description CVE ID	Patch	NCIIPC ID
Application(A)					
Apache					
Archiva *Apache Archiva is an extensible repository management software that helps taking care of your own personal or enterprise-wide build artifact repository.*					
Cross Site Scripting	28/07/2016	3.5	Cross-site scripting (XSS) vulnerability in Apache Archiva 1.3.9 and earlier allows remote authenticated administrators to inject arbitrary web script or HTML via the connector.sourceRepoId parameter to admin/addProxyConnector_commit.action. **Reference: CVE-2016-5005**	NA	A-APA-ARCHI-50816/01
Http Server *The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows.*					
NA	18/07/2016	5.1	The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other	https://www.apache.org/security/asf-httpoxy-response.txt	A-APA-HTTP - 50816/02

			words, this is not a CVE ID for a vulnerability. **Reference: CVE-2016-5387**		
Tomcat *Apache Tomcat, often referred to as Tomcat, is an open-source web server developed by the ApacheSoftware Foundation (ASF).*					
NA	18/07/2016	5.1	Apache Tomcat through 8.5.4, when the CGI Servlet is enabled, follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "A mitigation is planned for future releases of Tomcat, tracked as CVE-2016-5388"; in other words, this is not a CVE ID for a vulnerability. **Reference: CVE-2016-5388**	https://www.apache.org/security/asf-httpoxy-response.txt	A-APA-TOMCA--50816/03
Apple					
Safari *Safari is a web browser developed by Apple based on the WebKit engine.*					
NA	21/07/2016	5.8	Safari in Apple iOS before 9.3.3 allows remote attackers to spoof the displayed URL via an HTTP response specifying redirection to an invalid TCP port number. **Reference: CVE-2016-4604**	https://support.apple.com/HT206902	A-APP-SAFAR--50816/04
Safari;Webkit *Safari is a web browser developed by Apple based on the WebKit engine; WebKit is an open source web browser engine.*					
NA	21/07/2016	4.3	WebKit in Apple iOS before 9.3.3 and Safari before 9.1.2 mishandles about: URLs, which allows remote attackers to	https://support.apple.com/HT206902	A-APP-SAFAR--50816/05

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

			bypass the Same Origin Policy via a crafted web site. **Reference: CVE-2016-4590**		
Webkit *WebKit is an open source web browser engine.*					
Denial of Service	21/07/2016	7.1	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to cause a denial of service (memory consumption) via a crafted web site. **Reference: CVE-2016-4592**	https://support.apple.com/HT206905	A-APP-WEBKI--50816/06
NA	21/07/2016	7.8	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 mishandles the location variable, which allows remote attackers to access the local filesystem via unspecified vectors. **Reference: CVE-2016-4591**	https://support.apple.com/HT206905	A-APP-WEBKI--50816/07
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 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-2016-4622, CVE-2016-4623, and CVE-2016-4624. **Reference: CVE-2016-4589**	https://support.apple.com/HT206905	A-APP-WEBKI--50816/08
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	WebKit in Apple tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. **Reference: CVE-2016-4588**	https://support.apple.com/HT206905	A-APP-WEBKI--50816/09
Overflow; Gain Info	21/07/2016	4.3	WebKit in Apple iOS before 9.3.3 and tvOS before 9.2.2 allows remote attackers to obtain sensitive information from uninitialized process memory	https://support.apple.com/HT206905	A-APP-WEBKI--50816/10

			via a crafted web site. **Reference: CVE-2016-4587**		
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	WebKit in Apple Safari before 9.1.2 and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. **Reference: CVE-2016-4586**	https://support.apple.com/HT206905	A-APP-WEBKI--50816/11
Cross Site Scripting	21/07/2016	4.3	Cross-site scripting (XSS) vulnerability in the WebKit Page Loading implementation in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to inject arbitrary web script or HTML via an HTTP response specifying redirection that is mishandled by Safari. **Reference: CVE-2016-4585**	https://support.apple.com/HT206905	A-APP-WEBKI--50816/12
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	The WebKit Page Loading implementation in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. **Reference: CVE-2016-4584**	https://support.apple.com/HT206905	A-APP-WEBKI--50816/13
Bypass	21/07/2016	4.3	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to bypass the Same Origin Policy and obtain image date from an unintended web site via a timing attack involving an SVG document. **Reference: CVE-2016-4583**	https://support.apple.com/HT206905	A-APP-WEBKI--50816/14

CA

Ehealth

eHealth is a relatively recent term for healthcare practice supported by electronic processes and communication.

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; Execute Code	25/07/2016	9	CA eHealth 6.2.x and 6.3.x before 6.3.2.13 allows remote authenticated users to cause a denial of service or possibly execute arbitrary commands via unspecified vectors. **Reference: CVE-2016-6152**	http://www.ca.com/us/support/ca-support-online/product content/recommended-reading/security notices/ca20160721-01-security-notice-for-ca-ehealth.aspx	A-CA-EHEAL--50816/15
Denial of Service; Execute Code	25/07/2016	9	CA eHealth 6.2.x allows remote authenticated users to cause a denial of service or possibly execute arbitrary commands via unspecified vectors. **Reference: CVE-2016-6151**	http://www.ca.com/us/support/ca-support-online/product-content/recommended-reading/security-notices/ca20160721-01-security-notice-for-ca-ehealth.aspx	A-CA-EHEAL--50816/16
Ec-cube					
Coupon Plugin *JC Coupon is a WordPress Coupon Plugin which Allows You To Add Coupons on any post or page.*					
Execute Code; SQL Injection	31/07/2016	7.5	SQL injection vulnerability in the Seed Coupon plugin before 1.6 for EC-CUBE allows remote attackers to execute arbitrary SQL commands via unspecified vectors. **Reference: CVE-2016-4837**	http://www.ec-cube.net/products/detail.php?product_id=493	A-EC--COUPO--50816/17
Golang					
GO *Go is an open source programming language that makes it easy to build simple, reliable, and efficient software.*					
NA	18/07/2016	5.1	The net/http package in Go through 1.6 does not attempt to	https://bugzilla.redhat.com/s	A-GOL-GO--50816/18

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

			address RFC 3875 section 4.1.18 namespace conflicts and therefore does not protect CGI applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect a CGI application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. **Reference: CVE-2016-5386**	how_bug.cgi?id=1353798	
Google					
Chrome *Google Chrome is a freeware web browser developed by Google.*					
NA	23/07/2016	4.3	The CSPSource::schemeMatches function in WebKit/Source/core/frame/csp/CSPSource.cpp in the Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 52.0.2743.82, does not apply http :80 policies to https :443 URLs and does not apply ws :80 policies to wss :443 URLs, which makes it easier for remote attackers to determine whether a specific HSTS web site has been visited by reading a CSP report. NOTE: this vulnerability is associated with a specification change after CVE-2016-1617 resolution. **Reference: CVE-2016-5137**	http://googlechromereleases.blogspot.com/2016/07/stable-channel-update.html	A-GOO-CHROM--50816/19
Denial of Service	23/07/2016	6.8	Use-after-free vulnerability in extensions/renderer/user_script_injector.cc in the Extensions subsystem in Google Chrome before 52.0.2743.82 allows remote attackers to cause a	https://crbug.com/625393	A-GOO-CHROM--50816/20

			denial of service or possibly have unspecified other impact via vectors related to script deletion. **Reference: CVE-2016-5136**		
Bypass	23/07/2016	4.3	WebKit/Source/core/html/parser/HTMLPreloadScanner.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does not consider referrer-policy information inside an HTML document during a preload request, which allows remote attackers to bypass the Content Security Policy (CSP) protection mechanism via a crafted web site, as demonstrated by a "Content-Security-Policy: referrer origin-when-cross-origin" header that overrides a "<META name='referrer' content='no-referrer'>" element. **Reference: CVE-2016-5135**	https://crbug.com/605451	A-GOO-CHROM--50816/21
NA	23/07/2016	4.3	net/proxy/proxy_service.cc in the Proxy Auto-Config (PAC) feature in Google Chrome before 52.0.2743.82 does not ensure that URL information is restricted to a scheme, host, and port, which allows remote attackers to discover credentials by operating a server with a PAC script, a related issue to CVE-2016-3763. **Reference: CVE-2016-5134**	http://googlechromereleases.blogspot.com/2016/07/stable-channel-update.html	A-GOO-CHROM--50816/22
NA	23/07/2016	4.3	Google Chrome before 52.0.2743.82 mishandles origin information during proxy authentication, which allows man-in-the-middle attackers to spoof a proxy-authentication login prompt or trigger incorrect credential storage by	http://googlechromereleases.blogspot.com/2016/07/stable-channel-update.html	A-GOO-CHROM--50816/23

			modifying the client-server data stream. **Reference: CVE-2016-5133**		
Bypass	23/07/2016	6.8	The Service Workers subsystem in Google Chrome before 52.0.2743.82 does not properly implement the Secure Contexts specification during decisions about whether to control a subframe, which allows remote attackers to bypass the Same Origin Policy via an https IFRAME element inside an http IFRAME element. **Reference: CVE-2016-5132**	https://codereview.chromium.org/2082493002/	A-GOO-CHROM--50816/24
NA	23/07/2016	4.3	content/renderer/history_controller.cc in Google Chrome before 52.0.2743.82 does not properly restrict multiple uses of a JavaScript forward method, which allows remote attackers to spoof the URL display via a crafted web site. **Reference: CVE-2016-5130**	https://crbug.com/623319	A-GOO-CHROM--50816/25
Denial of Service	23/07/2016	6.8	Use-after-free vulnerability in WebKit/Source/core/editing/VisibleUnits.cpp in Blink, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code involving an @import at-rule in a Cascading Style Sheets (CSS) token sequence in conjunction with a rel=import attribute of a LINK element. **Reference: CVE-2016-5127**	https://codereview.chromium.org/2091633002	A-GOO-CHROM--50816/26
Denial of Service; Overflow	31/07/2016	6.8	Integer overflow in the kbasep_vinstr_attach_client function in midgard/mali_kbase_vinstr.c in	https://bugs.chromium.org/p/chromium/issues/detail?id	A-GOO-CHROM--50816/27

			Google Chrome before 52.0.2743.85 allows remote attackers to cause a denial of service (heap-based buffer overflow and use-after-free) by leveraging an unrestricted multiplication. **Reference: CVE-2016-5138**	=631752&desc=2	
Chrome;V8 *Google Chrome is a freeware web browser developed by Google; The V8 JavaScript Engine is an open source JavaScript engine developed by The Chromium Project for the Google Chrome web browser.*					
Denial of Service; Overflow Memory Corruption	23/07/2016	6.8	Google V8 before 5.2.361.32, as used in Google Chrome before 52.0.2743.82, does not properly process left-trimmed objects, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code. **Reference: CVE-2016-5129**	https://crbug.com/620553	A-GOO-CHROM--50816/28
Bypass	23/07/2016	6.8	objects.cc in Google V8 before 5.2.361.27, as used in Google Chrome before 52.0.2743.82, does not prevent API interceptors from modifying a store target without setting a property, which allows remote attackers to bypass the Same Origin Policy via a crafted web site. **Reference: CVE-2016-5128**	https://crbug.com/619166	A-GOO-CHROM--50816/29
Google;Xmlsoft					
Chrome/Libxml2 *Google Chrome is a freeware web browser developed by Google; libxml2 is a software library for parsing XML documents.*					
Denial of Service	23/07/2016	6.8	Use-after-free vulnerability in libxml2 through 2.9.4, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have	https://crbug.com/623378	A-GOO-CHROM--50816/30

			unspecified other impact via vectors related to the XPointer range-to function. **Reference: CVE-2016-5131**		
Icu Project					
International Components For Unicode *International Components for Unicode (ICU) is an open source project of mature C/C++ and Java libraries for Unicode support, software internationalization, and software globalization.*					
Denial of Service; Overflow	25/07/2016	7.5	The uloc_acceptLanguageFromHTTP function in common/uloc.cpp in International Components for Unicode (ICU) through 57.1 for C/C++ does not ensure that there is a '\0' character at the end of a certain temporary array, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long httpAcceptLanguage argument. **Reference: CVE-2016-6293**		A-ICU-INTER--50816/31
Intel					
Crosswalk *Crosswalk is a HTML5 runtime, built on open source foundations, which extends the web platform with new capabilities.*					
NA	31/07/2016	5.8	Intel Crosswalk before 19.49.514.5, 20.x before 20.50.533.11, 21.x before 21.51.546.0, and 22.x before 22.51.549.0 interprets a user's acceptance of one invalid X.509 certificate to mean that all invalid X.509 certificates should be accepted without prompting, which makes it easier for man-in-the-middle attackers to spoof SSL servers and obtain sensitive information via a crafted certificate. **Reference: CVE-2016-5672**	https://blogs.intel.com/evangelists/2016/07/28/crosswalk-security-vulnerability/	A-INT-CROSS--50816/32
Misys					

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

Fusioncapital Opics Plus *MISYS Fusion Capital Opics is the .NET service-oriented Treasury and Capital Markets solution with unsurpassed STP and back-office capabilities.*					
NA	19/07/2016	4.3	Misys FusionCapital Opics Plus does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to obtain sensitive information via a crafted certificate. **Reference: CVE-2016-5655**	http://www.kb.cert.org/vuls/id/682704	A-MIS-FUSIO--50816/33
NA	19/07/2016	8.5	Misys FusionCapital Opics Plus allows remote authenticated users to gain privileges via a man-in-the-middle attack that modifies the xmlMessageOut parameter. **Reference: CVE-2016-5654**	http://www.kb.cert.org/vuls/id/682704	A-MIS-FUSIO--50816/34
Execute Code; SQL Injection	19/07/2016	4	Multiple SQL injection vulnerabilities in Misys FusionCapital Opics Plus allow remote authenticated users to execute arbitrary SQL commands via the (1) ID or (2) Branch parameter. **Reference: CVE-2016-5653**	http://www.kb.cert.org/vuls/id/682704	A-MIS-FUSIO--50816/35
Objective Systems					
Asn1c *ASN1C ASN.1 Compiler Objective Systems' ASN1C compiler translates ASN.1 and/or XML schema (XSD) source specifications into C, C++, C#, or Java source code.*					
Denial of Service; Execute Code; Overflow	19/07/2016	10	Integer overflow in the rtxMemHeapAlloc function in asn1rt_a.lib in Objective Systems ASN1C for C/C++ before 7.0.2 allows context-dependent attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow), on a system running an application compiled by ASN1C, via crafted ASN.1 data. **Reference: CVE-2016-5080**	NA	A-OBJ-ASN1C--50816/36
Oracle					

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

Agile Product Lifecycle Management Framework *With Oracle's easy-to-use product lifecycle management solutions, you can accelerate time-to-market, reduce costs, and increase profitability.*					
NA	21/07/2016	3.5	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote authenticated users to affect confidentiality via vectors related to File Folders / Attachment, a different vulnerability than CVE-2016-3537. **Reference: CVE-2016-5473**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-AGILE--50816/37
Communications Eagle Application Processor *NA*					
NA	21/07/2016	5.5	Unspecified vulnerability in the Oracle Communications EAGLE Application Processor component in Oracle Communications Applications 16.0 allows remote authenticated users to affect confidentiality and integrity via vectors related to APPL. **Reference: CVE-2016-5458**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-COMMU--50816/38
Communications Messaging Server *The Oracle Communications Messaging Server provides a highly scalable, reliable, and available platform for delivering secure communication services.*					
NA	21/07/2016	5	Unspecified vulnerability in the Oracle Communications Messaging Server component in Oracle Communications Applications 6.3, 7.0, and 8.0 allows remote attackers to affect confidentiality via vectors related to Multiplexor. **Reference: CVE-2016-5455**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-COMMU--50816/39
Glassfish Server *Oracle GlassFish Server is the world's first implementation of the Java Platform, Enterprise Edition (Java EE) 6 specification.*					
NA	21/07/2016	5	Unspecified vulnerability in the Oracle GlassFish Server	http://www.oracle.com/techn	A-ORA-GLASS--

			component in Oracle Fusion Middleware 2.1.1 and 3.0.1 allows remote attackers to affect confidentiality via vectors related to Administration. **Reference: CVE-2016-5477**	etwork/security-advisory/cpujul2016-2881720.html	50816/40
Mysql *MySQL is an open-source relational database management system (RDBMS).*					
NA	21/07/2016	4.3	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows remote attackers to affect confidentiality via vectors related to Server: Connection. **Reference: CVE-2016-5444**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-MYSQL--50816/41
NA	21/07/2016	1.2	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows local users to affect availability via vectors related to Server: Connection. **Reference: CVE-2016-5443**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-MYSQL--50816/42
NA	21/07/2016	4	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Security: Encryption. **Reference: CVE-2016-5442**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-MYSQL--50816/43
NA	21/07/2016	4	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Replication. **Reference: CVE-2016-5441**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-MYSQL--50816/44
NA	21/07/2016	4	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier allows remote administrators to affect availability via vectors related	http://www.oracle.com/technetwork/security-advisory/cpujul2016-	A-ORA-MYSQL--50816/45

			to Server: RBR. **Reference: CVE-2016-5440**	2881720.html	
NA	21/07/2016	4	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Privileges. **Reference: CVE-2016-5439**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-MYSQL--50816/46
NA	21/07/2016	4	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Log. **Reference: CVE-2016-5437**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-MYSQL--50816/47
NA	21/07/2016	4	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: InnoDB. **Reference: CVE-2016-5436**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-MYSQL--50816/48
Peoplesoft Enterprise Peopletools *PeopleTools is the proprietary software development environment that was created by the PeopleSoft Corporation. The PeopleTools consist of Application Designer, Application Engine, Data Mover, PeopleCode and various other developer tools.*					
NA	21/07/2016	7.2	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.54 and 8.55 allows local users to affect confidentiality, integrity, and availability via vectors related to Install and Packaging. **Reference: CVE-2016-5472**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-PEOPL--50816/49
NA	21/07/2016	7.1	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.54 and 8.55 allows remote attackers to affect confidentiality via vectors	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-PEOPL--50816/50

			related to Application Designer. **Reference: CVE-2016-5470**		
NA	21/07/2016	5.8	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53, 8.54, and 8.55 allows remote attackers to affect confidentiality and integrity via vectors related to Panel Processor. **Reference: CVE-2016-5465**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-PEOPL--50816/51
Peoplesoft Enterprise Scm Eprocurement *PeopleSoft eProcurement helps enforce contract purchasing as well as capture spending information for future analysis.*					
NA	21/07/2016	5.5	Unspecified vulnerability in the PeopleSoft Enterprise FSCM component in Oracle PeopleSoft Products 9.1 and 9.2 allows remote authenticated users to affect confidentiality and integrity via vectors related to eProcurement. **Reference: CVE-2016-5467**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-PEOPL--50816/52
Retail Integration Bus *Oracle Retail Integration Bus (RIB) supports near-real-time messaging with guaranteed once-only delivery, guaranteed sequential delivery within a message family regardless of errors, automatic retry, the ability to fix and retry messages, multi-threading, and support for fast delivery of retail volumes.*					
NA	21/07/2016	6.5	Unspecified vulnerability in the Oracle Retail Integration Bus component in Oracle Retail Applications 13.0, 13.1, 13.2, 14.0, 14.1, and 15.0 allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to Install. **Reference: CVE-2016-5476**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-RETAI--50816/53
Retail Service Backbone *The Retail Service Backbone (RSB) is the product that defines the Oracle Retail Enterprise SOA Architecture and provides the infrastructure for the Services domain.*					
NA	21/07/2016	8	Unspecified vulnerability in the Oracle Retail Service Backbone	http://www.oracle.com/techn	A-ORA-RETAI--

			component in Oracle Retail Applications 14.0, 14.1, and 15.0 allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to Install. **Reference: CVE-2016-5475**	etwork/security-advisory/cpujul2016-2881720.html	50816/54
NA	21/07/2016	9	Unspecified vulnerability in the Oracle Retail Service Backbone component in Oracle Retail Applications 14.0, 14.1, and 15.0 allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to RSB Kernel. **Reference: CVE-2016-5474**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-RETAI--50816/55
Siebel Core-common Components *NA*					
NA	21/07/2016	4.3	Unspecified vulnerability in the Siebel Core - Common Components component in Oracle Siebel CRM 8.1.1, 8.2.2, IP2014, IP2015, and IP2016 allows remote attackers to affect integrity via vectors related to iHelp. **Reference: CVE-2016-5459**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-SIEBE--50816/56
Siebel Core-server Framework *The Siebel Core framework consists of Server infrastructure, Workflow engine, Scripting engine, Task-based UI engine, Workflow policies engine, Rules engine and Siebel Tools.*					
NA	21/07/2016	4.3	Unspecified vulnerability in the Siebel Core - Server Framework component in Oracle Siebel CRM 8.1.1, 8.2.2, IP2014, IP2015, and IP2016 allows remote attackers to affect confidentiality via vectors related to Services, a different vulnerability than CVE-2016-3450 and CVE-2016-5460.	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-SIEBE--50816/57

			Reference: CVE-2016-5466		
	21/07/2016	4	Unspecified vulnerability in the Siebel Core - Server Framework component in Oracle Siebel CRM 8.1.1, 8.2.2, IP2014, IP2015, and IP2016 allows remote administrators to affect confidentiality via vectors related to Workspaces. **Reference: CVE-2016-5462**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-SIEBE--50816/58
NA	21/07/2016	4	Unspecified vulnerability in the Siebel Core - Server Framework component in Oracle Siebel CRM 8.1.1, 8.2.2, IP2014, IP2015, and IP2016 allows remote authenticated users to affect confidentiality via vectors related to Object Manager. **Reference: CVE-2016-5461**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-SIEBE--50816/59
NA	21/07/2016	4.3	Unspecified vulnerability in the Siebel Core - Server Framework component in Oracle Siebel CRM 8.1.1, 8.2.2, IP2014, IP2015, and IP2016 allows remote attackers to affect confidentiality via vectors related to Services, a different vulnerability than CVE-2016-3450 and CVE-2016-5466. **Reference: CVE-2016-5460**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-SIEBE--50816/60
NA	21/07/2016	6.3	Unspecified vulnerability in the Siebel Core - Server Framework component in Oracle Siebel CRM 8.1.1, 8.2.2, IP2014, IP2015, and IP2016 allows remote authenticated users to affect confidentiality via vectors related to Services. **Reference: CVE-2016-5456**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-SIEBE--50816/61

Siebel Ui Framework

Siebel Open UI is an open architecture that you can use to customize the user interface that your enterprise

uses to display business process information.					
NA	21/07/2016	5.5	Unspecified vulnerability in the Siebel UI Framework component in Oracle Siebel CRM 8.1.1, 8.2.2, IP2014, IP2015, and IP2016 allows remote authenticated users to affect confidentiality and integrity via vectors related to EAI, a different vulnerability than CVE-2016-5451. **Reference: CVE-2016-5468**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-SIEBE--50816/62
Siebel Ui Framework *Siebel Open UI is an open architecture that you can use to customize the user interface that your enterprise uses to display business process information.*					
NA	21/07/2016	3.5	Unspecified vulnerability in the Siebel UI Framework component in Oracle Siebel CRM 8.1.1, 8.2.2, IP2014, IP2015, and IP2016 allows remote authenticated users to affect integrity via vectors related to SWSE Server, a different vulnerability than CVE-2016-5463. **Reference: CVE-2016-5464**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-SIEBE--50816/63
NA	21/07/2016	3.5	Unspecified vulnerability in the Siebel UI Framework component in Oracle Siebel CRM 8.1.1, 8.2.2, IP2014, IP2015, and IP2016 allows remote authenticated users to affect integrity via vectors related to SWSE Server, a different vulnerability than CVE-2016-5464. **Reference: CVE-2016-5463**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-SIEBE--50816/64
NA	21/07/2016	5.5	Unspecified vulnerability in the Siebel UI Framework component in Oracle Siebel CRM 8.1.1, 8.2.2, IP2014, IP2015, and IP2016 allows remote authenticated users to	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-SIEBE--50816/65

			affect confidentiality and integrity via vectors related to EAI, a different vulnerability than CVE-2016-5468. **Reference: CVE-2016-5451**		
NA	21/07/2016	4.3	Unspecified vulnerability in the Siebel UI Framework component in Oracle Siebel CRM 8.1.1, 8.2.2, IP2014, IP2015, and IP2016 allows remote attackers to affect integrity via vectors related to UIF Open UI. **Reference: CVE-2016-5450**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	A-ORA-SIEBE--50816/66
PHP					
PHP *PHP is a general-purpose scripting language that is especially suited to server-side web development, in which case PHP generally runs on a web server.*					
NA	18/07/2016	5.1	PHP through 7.0.8 does not attempt to address RFC 3875 section 4.1.18 namespace conflicts and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, as demonstrated by (1) an application that makes a getenv('HTTP_PROXY') call or (2) a CGI configuration of PHP, aka an "httpoxy" issue. **Reference: CVE-2016-5385**	https://bugzilla.redhat.com/show_bug.cgi?id=1353794	A-PHP-PHP--50816/67
Denial of Service; Overflow	25/07/2016	6.8	Integer overflow in the php_stream_zip_opener function in ext/zip/zip_stream.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to	https://bugs.php.net/72520	A-PHP-PHP--50816/68

			cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted zip:// URL. **Reference: CVE-2016-6297**		
Denial of Service; Overflow	25/07/2016	7.5	Integer signedness error in the simplestring_addn function in simplestring.c in xmlrpc-epi through 0.54.2, as used in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a long first argument to the PHP xmlrpc_encode_request function. **Reference: CVE-2016-6296**	https://bugs.php.net/72606	A-PHP-PHP--50816/69
Denial of Service	25/07/2016	7.5	ext/snmp/snmp.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773. **Reference: CVE-2016-6295**	https://bugs.php.net/72479	A-PHP-PHP--50816/70
Denial of Service	25/07/2016	7.5	The locale_accept_from_http function in ext/intl/locale/locale_methods.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU uloc_acceptLanguageFromHTTP function, which allows remote	https://bugs.php.net/72533	A-PHP-PHP--50816/71

			attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long argument. **Reference: CVE-2016-6294**		
Denial of Service	25/07/2016	4.3	The exif_process_user_comment function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted JPEG image. **Reference: CVE-2016-6292**	https://bugs.php.net/72618	A-PHP-PHP--50816/72
Denial of Service; Overflow Memory Corruption; Gain Information	25/07/2016	7.5	The exif_process_IFD_in_MAKERNOTE function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds array access and memory corruption), obtain sensitive information from process memory, or possibly have unspecified other impact via a crafted JPEG image. **Reference: CVE-2016-6291**	https://bugs.php.net/72603	A-PHP-PHP--50816/73
Denial of Service	25/07/2016	7.5	ext/session/session.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization. **Reference: CVE-2016-6290**	https://bugs.php.net/72562	A-PHP-PHP--50816/74
Denial of	25/07/2016	6.8	Integer overflow in the	https://bugs.ph	A-PHP-

Service; Overflow			virtual_file_ex function in TSRM/tsrm_virtual_cwd.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted extract operation on a ZIP archive. **Reference: CVE-2016-6289**	p.net/72513	PHP--50816/75
Denial of Service; Overflow	25/07/2016	7.5	The php_url_parse_ex function in ext/standard/url.c in PHP before 5.5.38 allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via vectors involving the smart_str data type. **Reference: CVE-2016-6288**	http://php.net/ChangeLog-5.php	A-PHP-PHP--50816/76
Rockwellautomation					
Factorytalk Energrymetrix *FactoryTalk EnergyMetrix is a web-enabled management software package that gives you access to critical energy information from virtually any location.*					
NA	27/07/2016	7.5	Rockwell Automation FactoryTalk EnergyMetrix before 2.20.00 does not invalidate credentials upon a logout action, which makes it easier for remote attackers to obtain access by leveraging an unattended workstation. **Reference: CVE-2016-4531**	https://ics-cert.us-cert.gov/advisories/ICSA-16-173-03	A-ROC-FACTO--50816/77
Execute Code; SQL Injection	27/07/2016	7.5	SQL injection vulnerability in Rockwell Automation FactoryTalk EnergyMetrix before 2.20.00 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. **Reference: CVE-2016-4522**	https://ics-cert.us-cert.gov/advisories/ICSA-16-173-03	A-ROC-FACTO--50816/78
Siemens					
Simatic Batch;Simatic Openpcs 7;Simatic Wincc					

The SIMATIC BATCH software can be used to implement even the most complex batch processes effectively and at a reasonable cost; OpenPCS V.7 is the version of our IEC 61131-3-compliant programming environment for the development of control applications which has proven its worth on the market; SIMATIC WinCC is a supervisory control and data acquisition (SCADA) and human-machine interface (HMI) system from Siemens.					
Exec Code	22/07/2016	10	Siemens SIMATIC WinCC before 7.3 Update 10 and 7.4 before Update 1, SIMATIC BATCH before 8.1 SP1 Update 9 as distributed in SIMATIC PCS 7 through 8.1 SP1, SIMATIC OpenPCS 7 before 8.1 Update 3 as distributed in SIMATIC PCS 7 through 8.1 SP1, SIMATIC OpenPCS 7 before 8.2 Update 1 as distributed in SIMATIC PCS 7 8.2, and SIMATIC WinCC Runtime Professional before 13 SP1 Update 9 allow remote attackers to execute arbitrary code via crafted packets. **Reference: CVE-2016-5743**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-378531.pdf	A-SIE-SIMAT--50816/79
Simatic Net Pc-software *The SIMATIC NET PC Software der Edition 2008 is released for use in SIMOTION applications.*					
Denial of Service	22/07/2016	5	Siemens SIMATIC NET PC-Software before 13 SP2 allows remote attackers to cause a denial of service (OPC UA service outage) via crafted TCP packets. **Reference: CVE-2016-5874**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-453276.pdf	A-SIE-SIMAT--50816/80
Simatic Wincc *SIMATIC WinCC is a supervisory control and data acquisition (SCADA) and human-machine interface (HMI) system from Siemens.*					
	22/07/2016	5	Siemens SIMATIC WinCC 7.0 through SP3 and 7.2 allows remote attackers to read arbitrary WinCC station files via crafted packets. **Reference: CVE-2016-5744**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-378531.pdf	A-SIE-SIMAT--50816/81
Sinema Remote Connect Server *The new management platform for remote networks, SINEMA Remote Connect, is a server application. SINEMA Remote Connect provides users access to remote plants or machines for convenient and secure maintenance.*					

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

XSS	22/07/2016	4.3	Cross-site scripting (XSS) vulnerability in the integrated web server in Siemens SINEMA Remote Connect Server before 1.2 allows remote attackers to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-6204**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-119132.pdf	A-SIE-SINEM--50816/82
Vtiger					
CRM *Vtiger CRM is a popular open source CRM application developed by the company Vtiger.*					
NA	31/07/2016	5.5	modules/Users/actions/Save.php in Vtiger CRM 6.4.0 and earlier does not properly restrict user-save actions, which allows remote authenticated users to create or modify user accounts via unspecified vectors. **Reference: CVE-2016-4834**	http://code.vtiger.com/vtiger/vtigercrm/commit/7cdf9941197b4aa58114eafce3ce88fb418eb68c	A-VTI-CRM--50816/83
Xmlsoft					
Libxml2 *libxml2 is a software library for parsing XML documents.*					
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	libxml2 in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4614, CVE-2016-4615, and CVE-2016-4616. **Reference: CVE-2016-4619**	https://support.apple.com/HT206905	A-XML-LIBXM--50816/84
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	libxml2 in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2	https://support.apple.com/HT206905	A-XML-LIBXM--50816/85

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 cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4614, CVE-2016-4615, and CVE-2016-4619. **Reference: CVE-2016-4616**		
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	libxml2 in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4614, CVE-2016-4616, and CVE-2016-4619. **Reference: CVE-2016-4615**	https://support.apple.com/HT206905	A-XML-LIBXM--50816/86
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	libxml2 in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4615, CVE-2016-4616, and CVE-2016-4619. **Reference: CVE-2016-4614**	https://support.apple.com/HT206905	A-XML-LIBXM--50816/87
Libxslt *Libxslt is the XSLT C library developed for the GNOME project. XSLT itself is a an XML language to define transformation for XML.*					
Denial of	21/07/2016	7.5	libxslt in Apple iOS before 9.3.3,	https://support.	A-XML-

Service; Overflow Memory Corruption			OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4607, CVE-2016-4608, CVE-2016-4609, and CVE-2016-4610. **Reference: CVE-2016-4612**	apple.com/HT206905	LIBXS--50816/88
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	libxslt in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4607, CVE-2016-4608, CVE-2016-4609, and CVE-2016-4612. **Reference: CVE-2016-4610**	https://support.apple.com/HT206905	A-XML-LIBXS--50816/89
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	libxslt in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-	https://support.apple.com/HT206905	A-XML-LIBXS--50816/90

			4607, CVE-2016-4608, CVE-2016-4610, and CVE-2016-4612. **Reference: CVE-2016-4609**		
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	libxslt in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4607, CVE-2016-4609, CVE-2016-4610, and CVE-2016-4612. **Reference: CVE-2016-4608**	https://support.apple.com/HT206904	A-XML-LIBXS--50816/91
Denial of Service; Overflow Memory Corruption	21/07/2016	7.5	libxslt in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4608, CVE-2016-4609, CVE-2016-4610, and CVE-2016-4612. **Reference: CVE-2016-4607**	https://support.apple.com/HT206905	A-XML-LIBXS--50816/92
Application;Operating System(A/OS)					
Apple/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	21/07/2016	6.8	WebKit in Apple iOS before 9.3.3,	https://support	A-OS-APP-

Service; Execute Code; Overflow; Memory Corruption			Safari before 9.1.2, and tvOS before 9.2.2 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-2016-4589, CVE-2016-4622, and CVE-2016-4623. **Reference: CVE-2016-4624**	.apple.com/HT206905	APPLE--50816/93
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 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-2016-4589, CVE-2016-4622, and CVE-2016-4624. **Reference: CVE-2016-4623**	https://support.apple.com/HT206905	A-OS-APP-APPLE--50816/94
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 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-2016-4589, CVE-2016-4623, and CVE-2016-4624. **Reference: CVE-2016-4622**	https://support.apple.com/HT206905	A-OS-APP-APPLE--50816/95
Cross Site Scripting	21/07/2016	4.3	Cross-site scripting (XSS) vulnerability in the WebKit JavaScript bindings in Apple iOS before 9.3.3 and Safari before 9.1.2 allows remote attackers to inject arbitrary web script or HTML via a crafted HTTP/0.9 response, related to a "cross-protocol cross-site scripting (XPXSS)" vulnerability. **Reference: CVE-2016-4651**	https://support.apple.com/HT206902	A-OS-APP-IPHON--50816/96

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

Canonical/Ecryptfs					
Ubuntu Linux/Ecryptfs-utils *Ubuntu is a Debian-based Linux operating system and distribution for personal computers, smartphones and network servers/ The ecryptfs-utils package provides several different ways of setting up eCryptfs.*					
NA	22/07/2016	2.1	ecryptfs-setup-swap in eCryptfs does not prevent the unencrypted swap partition from activating during boot when using GPT partitioning on a (1) NVMe or (2) MMC drive, which allows local users to obtain sensitive information via unspecified vectors. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-8946. **Reference: CVE-2016-6224**	https://bazaar.launchpad.net/~ecryptfs/ecryptfs/trunk/revision/882	A-OS-CAN-UBUNT--50816/97
Operating System(OS)					
Apple					
Apple Tv;Iphone Os;Mac Os X;Watchos *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 (originally Mac OS X) is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc; watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.*					
Denial of Service; Overflow; Gain Privileges; Memory Corruption	21/07/2016	7.2	The kernel in Apple iOS before 9.3.3, OS X before 10.11.6, tvOS before 9.2.2, and watchOS before 2.2.2 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1863 and CVE-2016-4582. **Reference: CVE-2016-4653**	https://support.apple.com/HT206905	O-APP-APPLE--50816/98
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	CoreGraphics in Apple iOS before 9.3.3, OS X before 10.11.6, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted BMP image.	https://support.apple.com/HT206905	O-APP-APPLE--50816/99

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-2016-4637		
Denial of Service; Overflow	21/07/2016	5	ImageIO in Apple iOS before 9.3.3, OS X before 10.11.6, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors. **Reference: CVE-2016-4632**	https://support.apple.com/HT206905	O-APP-APPLE--50816/100
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	ImageIO in Apple iOS before 9.3.3, OS X before 10.11.6, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted TIFF file. **Reference: CVE-2016-4631**	https://support.apple.com/HT206905	O-APP-APPLE--50816/101
Denial of Service; Gain Privileges	21/07/2016	7.2	IOHIDFamily in Apple iOS before 9.3.3, OS X before 10.11.6, tvOS before 9.2.2, and watchOS before 2.2.2 allows local users to gain privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors. **Reference: CVE-2016-4626**	https://support.apple.com/HT206905	O-APP-APPLE--50816/102
NA	21/07/2016	4.6	The Sandbox Profiles component in Apple iOS before 9.3.3, OS X before 10.11.6, tvOS before 9.2.2, and watchOS before 2.2.2 allows attackers to access the process list via a crafted app that makes an API call. **Reference: CVE-2016-4594**	https://support.apple.com/HT206905	O-APP-APPLE--50816/103
Denial of Service; Overflow Gain Privileges; Memory Corruption	21/07/2016	7.2	The kernel in Apple iOS before 9.3.3, OS X before 10.11.6, tvOS before 9.2.2, and watchOS before 2.2.2 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-	https://support.apple.com/HT206904	O-APP-APPLE--50816/104

			1863 and CVE-2016-4653. **Reference: CVE-2016-4582**		
Denial of Service; Gain Privileges	21/07/2016	7.2	IOAcceleratorFamily in Apple iOS before 9.3.3, tvOS before 9.2.2, and watchOS before 2.2.2 allows local users to gain privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors. **Reference: CVE-2016-4627**	https://support.apple.com/HT206905	O-APP-APPLE--50816/105
Iphone Os *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware*					
Denial of Service	21/07/2016	7.1	Calendar in Apple iOS before 9.3.3 allows remote attackers to cause a denial of service (NULL pointer dereference and device restart) via a crafted invitation. **Reference: CVE-2016-4605**	https://support.apple.com/HT206902	O-APP-IPHON--50816/106
Bypass; Gain Information	21/07/2016	4.3	Web Media in Apple iOS before 9.3.3 allows attackers to bypass the Private Browsing protection mechanism and obtain sensitive video URL information by leveraging Safari View Controller misbehavior. **Reference: CVE-2016-4603**	https://support.apple.com/HT206902	O-APP-IPHON--50816/107
	21/07/2016	2.1	The Siri Contacts component in Apple iOS before 9.3.3 allows physically proximate attackers to read arbitrary Contact card information via unspecified vectors. **Reference: CVE-2016-4593**	https://support.apple.com/HT206902	O-APP-IPHON--50816/108
Iphone Os;Mac Os X *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware; OS X (originally Mac OS X) is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc*					
NA	21/07/2016	3.5	FaceTime in Apple iOS before 9.3.3 and OS X before 10.11.6 allows man-in-the-middle attackers to spoof relayed-call	https://support.apple.com/HT206903	O-APP-IPHON--50816/109

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

			termination, and obtain sensitive audio information in opportunistic circumstances, via unspecified vectors. **Reference: CVE-2016-4635**		
Iphone Os;Watchos *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware; watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.*					
Denial of service; Gain Information	21/07/2016	4.9	IOAcceleratorFamily in Apple iOS before 9.3.3 and watchOS before 2.2.2 allows local users to obtain sensitive information from kernel memory or cause a denial of service (out-of-bounds read) via unspecified vectors. **Reference: CVE-2016-4628**	https://support.apple.com/HT206904	O-APP-IPHON--50816/110
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.*					
Denial of Service; Gain Privileges; Gain Information	21/07/2016	3.3	CoreGraphics in Apple OS X before 10.11.6 allows local users to obtain sensitive information from kernel memory and consequently gain privileges, or cause a denial of service (out-of-bounds read), via unspecified vectors. **Reference: CVE-2016-4652**	https://support.apple.com/HT206903	O-APP-MACO--50816/111
Denial of Service	21/07/2016	2.1	Audio in Apple OS X before 10.11.6 allows local users to cause a denial of service (NULL pointer dereference) via unspecified vectors. **Reference: CVE-2016-4649**	https://support.apple.com/HT206903	O-APP-MACO--50816/112
Denial of service; Gain Information	21/07/2016	4.9	Audio in Apple OS X before 10.11.6 allows local users to obtain sensitive kernel memory-layout information or cause a denial of service (out-of-bounds read) via unspecified vectors. **Reference: CVE-2016-4648**	https://support.apple.com/HT206903	O-APP-MACO--50816/113
Denial of	21/07/2016	7.2	Audio in Apple OS X before	https://suppor	O-APP-MAC

Service; Overflow; Gain Privileges; Memory Corruption			10.11.6 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted file. **Reference: CVE-2016-4647**	t.apple.com/HT 206903	O-- 50816/114
Denial of service; Gain Information	21/07/2016	4.3	Audio in Apple OS X before 10.11.6 mishandles a size value, which allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read) via a crafted audio file. **Reference: CVE-2016-4646**	https://support.apple.com/HT 206903	O-APP-MAC O-- 50816/115
NA	21/07/2016	2.1	CFNetwork in Apple OS X before 10.11.6 uses weak permissions for web-browser cookies, which allows local users to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-4645**	https://support.apple.com/HT 206903	O-APP-MAC O-- 50816/116
Execute Code; Gain Information	21/07/2016	9.3	Login Window in Apple OS X before 10.11.6 allows attackers to execute arbitrary code in a privileged context or obtain sensitive user information via a crafted app that leverages a "type confusion." **Reference: CVE-2016-4641**	https://support.apple.com/HT 206903	O-APP-MAC O-- 50816/117
Dejnial of Service; Execute Code; Overflow; Memory Corruption; Gain Information	21/07/2016	9.3	Login Window in Apple OS X before 10.11.6 allows attackers to execute arbitrary code in a privileged context, obtain sensitive user information, or cause a denial of service (memory corruption) via a crafted app. **Reference: CVE-2016-4640**	https://support.apple.com/HT 206903	O-APP-MAC O-- 50816/118
Denial of Service	21/07/2016	4.4	Login Window in Apple OS X before 10.11.6 does not properly initialize memory, which allows local users to cause a denial of service via unspecified vectors. **Reference: CVE-2016-4639**	https://support.apple.com/HT 206903	O-APP-MAC O-- 50816/119

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

NA	21/07/2016	9.3	Login Window in Apple OS X before 10.11.6 allows attackers to gain privileges via a crafted app that leverages a "type confusion." **Reference: CVE-2016-4638**	https://support.apple.com/HT206903	O-APP-MACO--50816/120
Denial of Service; Overflow; Gain Privileges; Memory Corruption	21/07/2016	7.2	The Graphics Drivers subsystem in Apple OS X before 10.11.6 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors. **Reference: CVE-2016-4634**	https://support.apple.com/HT206903	O-APP-MACO--50816/121
Denial of Service; Execute Code; Memory Corruption	21/07/2016	6.9	Intel Graphics Driver in Apple OS X before 10.11.6 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference: CVE-2016-4633**	https://support.apple.com/HT206903	O-APP-MACO--50816/122
DoS Exec Code Overflow Mem. Corr.	21/07/2016	6.8	ImageIO in Apple OS X before 10.11.6 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted EXR image with B44 compression. **Reference: CVE-2016-4630**	https://support.apple.com/HT206903	O-APP-MACO--50816/123
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	10	ImageIO in Apple OS X before 10.11.6 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted xStride and yStride values in an EXR image. **Reference: CVE-2016-4629**	https://support.apple.com/HT206903	O-APP-MACO--50816/124
NA	21/07/2016	7.2	Use-after-free vulnerability in IOSurface in Apple OS X before 10.11.6 allows local users to gain privileges via unspecified vectors. **Reference: CVE-2016-4625**	https://support.apple.com/HT206903	O-APP-MACO--50816/125

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; Execute Code; Overflow; Memory Corruption	21/07/2016	9.3	libc++abi in Apple OS X before 10.11.6 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference: CVE-2016-4621**	https://support.apple.com/HT206903	O-APP-MACO--50816/126
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	QuickTime in Apple OS X before 10.11.6 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted FlashPix bitmap image, a different vulnerability than CVE-2016-4596, CVE-2016-4597, and CVE-2016-4600. **Reference: CVE-2016-4602**	https://support.apple.com/HT206903	O-APP-MACO--50816/127
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	QuickTime in Apple OS X before 10.11.6 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted SGI image. **Reference: CVE-2016-4601**	https://support.apple.com/HT206903	O-APP-MACO--50816/128
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	QuickTime in Apple OS X before 10.11.6 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted FlashPix bitmap image, a different vulnerability than CVE-2016-4596, CVE-2016-4597, and CVE-2016-4602. **Reference: CVE-2016-4600**	https://support.apple.com/HT206903	O-APP-MACO--50816/129
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	QuickTime in Apple OS X before 10.11.6 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Photoshop document. **Reference: CVE-2016-4599**	https://support.apple.com/HT206903	O-APP-MACO--50816/130
Denial of Service;	21/07/2016	6.8	QuickTime in Apple OS X before 10.11.6 allows remote attackers	https://support.apple.com/H	O-APP-MACO--

Execute Code; Overflow; Memory Corruption			to execute arbitrary code or cause a denial of service (memory corruption) via a crafted image. **Reference: CVE-2016-4598**	T206903	50816/131
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	QuickTime in Apple OS X before 10.11.6 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted FlashPix bitmap image, a different vulnerability than CVE-2016-4596, CVE-2016-4600, and CVE-2016-4602. **Reference: CVE-2016-4597**	https://support.apple.com/HT206903	O-APP-MACO--50816/132
Denial of Service; Execute Code; Overflow; Memory Corruption	21/07/2016	6.8	QuickTime in Apple OS X before 10.11.6 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted FlashPix bitmap image, a different vulnerability than CVE-2016-4597, CVE-2016-4600, and CVE-2016-4602. **Reference: CVE-2016-4596**	https://support.apple.com/HT206903	O-APP-MACO--50816/133
NA	21/07/2016	2.1	Safari Login AutoFill in Apple OS X before 10.11.6 allows physically proximate attackers to discover passwords by reading the screen during the login procedure. **Reference: CVE-2016-4595**	https://support.apple.com/HT206903	O-APP-MACO--50816/134
Oracle					
Integrated Lights Out Manager Firmware *Oracle Integrated Lights Out Manager (ILOM) is the service processor embedded on all Oracle's SPARC Enterprise T-series and Sun Fire x86 servers, including all rack mounts and blades.*					
NA	21/07/2016	9	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	O-ORA-INTEG--50816/135

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

			to LUMAIN. **Reference: CVE-2016-5457**		
NA	21/07/2016	7.5	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to IPMI. **Reference: CVE-2016-5453**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	O-ORA-INTEG--50816/136
NA	21/07/2016	5	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect availability via vectors related to Console Redirection. **Reference: CVE-2016-5449**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	O-ORA-INTEG--50816/137
NA	21/07/2016	6.4	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect integrity and availability via vectors related to SNMP. **Reference: CVE-2016-5448**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	O-ORA-INTEG--50816/138
NA	21/07/2016	6.5	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors. **Reference: CVE-2016-5447**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	O-ORA-INTEG--50816/139
NA	21/07/2016	7.5	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via vectors related	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	O-ORA-INTEG--50816/140

			to Infrastructure. **Reference: CVE-2016-5446**		
NA	21/07/2016	7.5	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. **Reference: CVE-2016-5445**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	O-ORA-INTEG--50816/141
Solaris *Oracle Solaris Cluster provides high availability for enterprise applications and databases on theOracle Solaris OS.*					
NA	21/07/2016	2.1	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect availability via vectors related to Kernel, a different vulnerability than CVE-2016-3497 and CVE-2016-5469. **Reference: CVE-2016-5471**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	O-ORA-SOLAR--50816/142
NA	21/07/2016	2.1	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect availability via vectors related to Kernel, a different vulnerability than CVE-2016-3497 and CVE-2016-5471. **Reference: CVE-2016-5469**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	O-ORA-SOLAR--50816/143
NA	21/07/2016	5.4	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect integrity and availability via vectors related to Verified Boot. **Reference: CVE-2016-5454**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html	O-ORA-SOLAR--50816/144
NA	21/07/2016	2.1	Unspecified vulnerability in Oracle Sun Solaris 11.3 allows local users to affect confidentiality via vectors related to Verified Boot. **Reference: CVE-2016-5452**	http://www.oracle.com/technetwork/security-advisory/cpujul2016-	O-ORA-SOLAR--50816/145

				2881720.html	

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