National Critical Information Infrastructure Protection Centre

CVE Report

24 - 31 Jan 2016

Vol. 3 No.4

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Application(A)					
Apache					
Hive *Hive is a data warehouse infrastructure tool to process structured data in Hadoop. It resides on top of Hadoop to summarize Big Data, and makes querying and analyzing easy.*					
Bypass	29-Jan-16	7.5	The authorization framework in Apache Hive 1.0.0, 1.0.1, 1.1.0, 1.1.1, 1.2.0 and 1.2.1, on clusters protected by Ranger and SqlStdHiveAuthorization, allows attackers to bypass intended parent table access restrictions via unspecified partition-level operations. **Reference: CVE-2015-7521**	http://www.hive.org/security/2016/dsa-3458	A-APA-HIVE-310116/1
Cakephp					
Cakephp *Cakephp is an open-source web framework. It follows the model–view–controller (MVC) approach and is written in PHP.*					
Bypass; Cross-site Request Forgery	26-Jan-16	6.8	CakePHP 2.x and 3.x before 3.1.5 might allow remote attackers to bypass the CSRF protection mechanism via the _method parameter. **Reference: CVE-2015-8379**	http://bakery.cakephp.org/2015/11/29/cakephp_315_released.html	A-CAK-CAKEP-310116/2
Cisco					
Application Policy Infrastructure Controller Enterprise Module *The Cisco Application Policy Infrastructure Controller (APIC) Enterprise Module is a software controller that automates and simplifies network configuration*					
Cross Site Scripting	26-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) 1.0.10 allows remote attackers to inject arbitrary web script or HTML via a crafted hostname in an SNMP response, aka Bug ID CSCuw47238.	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160125-api	A-CIS-APPLI-310116/3

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Reference: CVE-2015-6337		
Unified Contact Center Express *Cisco Unified Contact Center Express is a single-server, integrated 'contact center in a box' for both formal and informal contact centers.*					
Cross Site Scripting	26-Jan-16	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Cisco Unified Contact Center Express 10.0(1), 10.5(1), 10.6(1), and 11.0(1) allow remote attackers to inject arbitrary web script or HTML via vectors related to permalinks, aka Bug ID CSCux92033. **Reference: CVE-2016-1298**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160125-ucce	A-CIS-UNIFI-310116/4
Unity Connection *Unity Connection is a voicemail and unified messaging platform with a comprehensive feature set and is based on the same Linux Unified Communications Operating System as Cisco Unified Communications Manager.*					
Cross Site Scripting	27-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in Cisco Unity Connection (UC) 10.5(2.3009) allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka Bug ID CSCux82582. **Reference: CVE-2016-1300**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160127-uc	A-CIS-UNITY-310116/5
Cross Site Scripting	30-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in Cisco Unity Connection 10.5(2.3009) allows remote attackers to inject arbitrary web script or HTML via a crafted value, aka Bug ID CSCux82596. **Reference: CVE-2016-1304**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160128-uc	A-CIS-UNITY-310116/6
Wide Area Application Services *Cisco Wide Area Application Services (WAAS) is technology developed by Cisco Systems that optimizes the performance of any TCP-based application operating in a wide area network (WAN) environment while preserving and strengthening branch security.*					
Denial of Service	27-Jan-16	7.8	cifs-ao in the CIFS optimization functionality on Cisco Wide Area Application Service (WAAS) and Virtual	http://tools.cisco.com/security/center/content/	A-CIS-WIDE-310116/7

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			WAAS (vWAAS) devices 5.x before 5.3.5d and 5.4 and 5.5 before 5.5.3 allows remote attackers to cause a denial of service (resource consumption and device reload) via crafted network traffic, aka Bug ID CSCus85330. **Reference: CVE-2015-6421**	CiscoSecurityAdvisory/cisco-sa-20160127-waascifs	
Debian					
Fuse *Filesystem in Userspace (FUSE) is a simple interface for userspace programs to export a virtual filesystem to the Linux kernel.*					
Gain Privileges	26-Jan-16	7.2	An unspecified udev rule in the Debian fuse package in jessie before 2.9.3-15+deb8u2, in stretch before 2.9.5-1, and in sid before 2.9.5-1 sets world-writable permissions for the /dev/cuse character device, which allows local users to gain privileges via a character device in /dev, related to an ioctl. **Reference: CVE-2016-1233**	http://www.debian.org/security/2016/dsa-3451	A-DEB-FUSE-310116/8
Golan					
GO *Go is an open source programming language created at Google in 2007*					
Gain Information	27-Jan-16	5	The Int.Exp Montgomery code in the math/big library in Go 1.5.x before 1.5.3 mishandles carry propagation and produces incorrect output, which makes it easier for attackers to obtain private RSA keys via unspecified vectors. **Reference: CVE-2015-8618**	https://go-review.googlesource.com/#/c/17672/	A-GOL-GO-310116/9
Google					
Chrome *Google Chrome is a browser that combines a minimal design with sophisticated technology to make the web faster, safer, and easier.*					

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Gain Information	25-Jan-16	4.3	The UnacceleratedImageBufferSurface class in WebKit/Source/platform/graphics/UnacceleratedImageBufferSurface.cpp in Blink, as used in Google Chrome before 48.0.2564.82, mishandles the initialization mode, which allows remote attackers to obtain sensitive information from process memory via a crafted web site. **Reference: CVE-2016-1614**	https://codereview.chromium.org/1407393002/	A-GOO-CHROM-310116/10
Gain Information	25-Jan-16	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 48.0.2564.82, does not apply http policies to https URLs and does not apply ws policies to wss URLs, which makes it easier for remote attackers to determine whether a specific HSTS web site has been visited by reading a CSP report. **Reference: CVE-2016-1617**	https://codereview.chromium.org/1455973003	A-GOO-CHROM-310116/11
Denial of Service	25-Jan-16	6.8	The LoadIC::UpdateCaches function in ic/ic.cc in Google V8, as used in Google Chrome before 48.0.2564.82, does not ensure receiver compatibility before performing a cast of an unspecified variable, which allows remote attackers to cause a denial of service or possibly have unknown other impact via crafted JavaScript code. **Reference: CVE-2016-1612**	http://googlechromereleases.blogspot.com/2016/01/stable-channel-update_20.html	A-GOO-CHROM-310116/12

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Denial of Service	2016-01-25	6.8	Multiple use-after-free vulnerabilities in the formfiller implementation in PDFium, as used in Google Chrome before 48.0.2564.82, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to improper tracking of the destruction of (1) IPWL_FocusHandler and (2) IPWL_Provider objects. **Reference: CVE-2016-1613**	http://googlechromereleases.blogspot.com/2016/01/stable-channel-update_20.html	A-GOO-CHROM-310116/13
Denial of Service	25-Jan-16	6.8	Multiple unspecified vulnerabilities in Google V8 before 4.8.271.17, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via unknown vectors. **Reference: CVE-2016-2051**	http://googlechromereleases.blogspot.com/2016/01/stable-channel-update_20.html	A-GOO-CHROM-310116/14
Denial of Service	25-Jan-16	9.3	Multiple unspecified vulnerabilities in Google Chrome before 48.0.2564.82 allow attackers to cause a denial of service or possibly have other impact via unknown vectors. **Reference: CVE-2016-1620**	http://googlechromereleases.blogspot.com/2016/01/stable-channel-update_20.html	A-GOO-CHROM-310116/15
Denial of Service; Overflow	25-Jan-16	6.8	Multiple integer overflows in the (1) sycc422_to_rgb and (2) sycc444_to_rgb functions in fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 48.0.2564.82, allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted PDF document. **Reference: CVE-2016-1619**	https://codereview.chromium.org/1521473003	A-GOO-CHROM-310116/16

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Not Available	25-Jan-16	4.3	The Omnibox implementation in Google Chrome before 48.0.2564.82 allows remote attackers to spoof a document's origin via unspecified vectors. **Reference: CVE-2016-1615**	http://googlechromereleases.blogspot.com/2016/01/stable-channel-update_20.html	A-GOO-CHROM-310116/17
Not Available	25-Jan-16	4.3	The CustomButton::AcceleratorPressed function in ui/views/controls/button/custom_button.cc in Google Chrome before 48.0.2564.82 allows remote attackers to spoof URLs via vectors involving an unfocused custom button. **Reference: CVE-2016-1616**	https://codereview.chromium.org/1437523005	A-GOO-CHROM-310116/18
Not Available	25-Jan-16	4.3	Blink, as used in Google Chrome before 48.0.2564.82, does not ensure that a proper cryptographicallyRandomValues random number generator is used, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors. **Reference: CVE-2016-1618**	https://codereview.chromium.org/1419293005	A-GOO-CHROM-310116/19
Google;Harfbuzz Project					
Chrome/Harfbuzz *Google Chrome is a browser that combines a minimal design with sophisticated technology to make the web faster, safer, and easier.; HarfBuzz is a software development library for text shaping, which is the process of converting Unicode text to glyph indices and positions.*					
Denial of Service	25-Jan-16	7.5	Multiple unspecified vulnerabilities in HarfBuzz before 1.0.6, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via unknown vectors. **Reference: CVE-2016-2052**	http://googlechromereleases.blogspot.com/2016/01/stable-channel-update_20.html	A-GOO-CHROM-310116/20

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

National Critical Information Infrastructure Protection Centre

CVE Report

24 - 31 Jan 2016

Vol. 3 No.4

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Haxx					
Curl *Curl is a computer software project providing a library and command-line tool for transferring data using various protocol*					
Not Available	29-Jan-16	5	cURL before 7.47.0 on Windows allows attackers to write to arbitrary files in the current working directory on a different drive via a colon in a remote file name. **Reference: CVE-2016-0754**	http://curl.haxx.se/docs/adv_20160127B.html	A-HAX-CURL-310116/21
HP					
Operations Manager *Operations management is an area of management concerned with designing, and controlling the process of production and redesigning business operations in the production of goods or services.*					
Execute Code	30-Jan-16	10	HPE Operations Manager 8.x and 9.0 on Windows allows remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections library. **Reference: CVE-2016-1985**	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04953244	A-HP-OPERA-310116/22
IBM					
Jazz Reporting Service *Jazz Reporting Service is an alternative to the complex reporting capabilities that are available in many Rational products and solutions.*					
Denial of Service	29-Jan-16	5	Report Builder in IBM Jazz Reporting Service (JRS) 5.x before 5.0.2-Rational-CLM-ifix011 and 6.0 before 6.0.0-Rational-CLM-ifix005 allows remote attackers to cause a denial of service (Report Builder server outage) via a crafted request to a Report Builder instance URL. **Reference: CVE-2015-7464**	http://www-01.ibm.com/support/docview.wss?uid=swg21972485	A-IBM-JAZZ-310116/23
Spectrum Scale *IBM Spectrum Scale is software-defined storage for high performance, large scale workloads on-premises or in the cloud.*					

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Gain Information	27-Jan-16	2.1	IBM Spectrum Scale 4.1.1.x before 4.1.1.4 and 4.2.x before 4.2.0.1, in certain LDAP File protocol configurations, allows remote attackers to discover an LDAP password via unspecified vectors. **Reference: CVE-2015-7488**	http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005580	A-IBM-SPECT-310116/24
Websphere Portal *IBM WebSphere Portal is a set of software tools that enables companies to build and manage web portals.*					
Cross Site Scripting	27-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in IBM WebSphere Portal 8.5.0 before CF09 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-0209**	http://www-01.ibm.com/support/docview.wss?uid=swg21974564	A-IBM-WEBSP-310116/25
Intel					
Driver Update Utility *The Intel Driver Update Utility helps keeps your system up-to-date by detecting when updates are available.*					
Execute Code	29-Jan-16	7.6	Intel Driver Update Utility before 2.4 retrieves driver updates in cleartext, which makes it easier for man-in-the-middle attackers to execute arbitrary code via a crafted file. **Reference: CVE-2016-1493**	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00048&languageid=en-fr	A-INT-DRIVE-310116/26
Lenovo					
Shareit *Shareit is a free file sharing app that works across multiple operating systems.*					
Gain Information	26-Jan-16	2.7	The Wifi hotspot in Lenovo SHAREit before 3.2.0 for Windows allows remote attackers to obtain sensitive file names via a crafted file request to /list. **Reference: CVE-2016-1490**	https://support.lenovo.com/us/en/product_security/len_4058	A-LEN-SHARE-310116/27
Gain Information	26-Jan-16	4.3	Lenovo SHAREit before 3.2.0 for Windows and SHAREit	https://support.lenovo	A-LEN-SHARE-

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			before 3.5.48_ww for Android transfer files in cleartext, which allows remote attackers to (1) obtain sensitive information by sniffing the network or (2) conduct man-in-the-middle (MITM) attacks via unspecified vectors. **Reference: CVE-2016-1489**	.com/us/en/product_security/len_4058	310116/28
Not Available	26-Jan-16	2.9	The Wifi hotspot in Lenovo SHAREit before 3.5.48_ww for Android, when configured to receive files, does not require a password, which makes it easier for remote attackers to obtain access by leveraging a position within the WLAN coverage area. **Reference: CVE-2016-1492**	https://support.lenovo.com/us/en/product_security/len_4058	A-LEN-SHARE-310116/29
Not Available	26-Jan-16	5.4	The Wifi hotspot in Lenovo SHAREit before 3.2.0 for Windows, when configured to receive files, has a hardcoded password of 12345678, which makes it easier for remote attackers to obtain access by leveraging a position within the WLAN coverage area. **Reference: CVE-2016-1491**	https://support.lenovo.com/us/en/product_security/len_4058	A-LEN-SHARE-310116/30
Mariadb					
Mariadb					
One of the most popular database servers. Made by the original developers of MySQL.					
Not Available	27-Jan-16	4.3	The ssl_verify_server_cert function in sql-common/client.c in MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10, Oracle MySQL, and Percona Server do not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows	https://mariadb.atlassian.net/browse/MDEV-9212	A-MAR-MARIA-310116/31

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			man-in-the-middle attackers to spoof SSL servers via a "/CN=" string in a field in a certificate, as demonstrated by "/OU=/CN=bar.com/CN=foo.com." **Reference: CVE-2016-2047**		
Matroska					
Libebml *EBML was designed to be a simplified binary extension of XML for the purpose of storing and manipulating data in a hierarchical form with variable field lengths.*					
Gain Information	29-Jan-16	4.3	The EbmlUnicodeString::UpdateFromUTF8 function in libEBML before 1.3.3 allows context-dependent attackers to obtain sensitive information from process heap memory via a crafted UTF-8 string, which triggers an invalid memory access. **Reference: CVE-2015-8790**	https://github.com/Matroska-Org/libebml/blob/release-1.3.3/ChangeLog	A-MAT-LIBEB-310116/32
Gain Information	29-Jan-16	4.3	The EbmlElement::ReadCodedSizeValue function in libEBML before 1.3.3 allows context-dependent attackers to obtain sensitive information from process heap memory via a crafted length value in an EBML id, which triggers an invalid memory access. **Reference: CVE-2015-8791**	https://github.com/Matroska-Org/libebml/commit/24e5cd7c666b1ddd85619d60486db0a5481c1b90	A-MAT-LIBEB-310116/33
Not Available	29-Jan-16	9.3	Use-after-free vulnerability in the EbmlMaster::Read function in libEBML before 1.3.3 allows context-dependent attackers to have unspecified impact via a "deeply nested element with infinite size" followed by another element of an upper level in an EBML document. **Reference: CVE-2015-8789**	https://github.com/Matroska-Org/libebml/blob/release-1.3.3/ChangeLog	A-MAT-LIBEB-310116/34

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Mcafee					
File Lock *File Locker is a light-weight and easy-to-use file lock software product for Windows. It can protect your private files*					
Denial of Service; Gain Information	29-Jan-16	8.5	McPvDrv.sys 4.6.111.0 in McAfee File Lock 5.x in McAfee Total Protection allows local users to obtain sensitive information from kernel memory or cause a denial of service (system crash) via a large VERIFY_INFORMATION.Length value in an IOCTL_DISK_VERIFY ioctl call. **Reference: CVE-2015-8772**		A-MCA-FILE -310116/35
Denial of Service; Overflow	29-Jan-16	7.8	Stack-based buffer overflow in McPvDrv.sys 4.6.111.0 in McAfee File Lock 5.x in McAfee Total Protection allows attackers to cause a denial of service (system crash) via a long vault GUID in an ioctl call. **Reference: CVE-2015-8773**		A-MCA-FILE -310116/36
Microsys					
Promotic *The promotic system is a software tool used for visualization and control of technological processes in a wide spectrum of industrial branches.*					
Denial of Service; Overflow	26-Jan-16	7.1	Heap-based buffer overflow in MICROSYS PROMOTIC before 8.3.11 allows remote authenticated users to cause a denial of service via a malformed HTML document. **Reference: CVE-2016-0869**	http://www.promotic.eu/en/pmdoc/NewsPm803.htm#ver80311	A-MIC-PROMO-310116/37
Mozilla					
Firefox *Mozilla Firefox, a free Web browser. Firefox is created by a global non-profit dedicated to putting individuals in control online.*					
Gain Information	31-Jan-16	5	Mozilla Firefox before 44.0 stores cookies with names containing vertical tab characters, which allows	https://bugzilla.mozilla.org/show_bug.cgi?	A-MOZ-FIREF-310116/38

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			remote attackers to obtain sensitive information by reading HTTP Cookie headers. NOTE: this vulnerability exists because of an incomplete fix for **Reference: CVE-**2015-7208. **Reference: CVE-2016-1939**	id=1233784	
Denial of Service	31-Jan-16	9.3	The nsZipArchive function in Mozilla Firefox before 44.0 might allow remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect use of a pointer during processing of a ZIP archive. **Reference: CVE-2016-1945**	https://bugzilla.mozilla.org/show_bug.cgi?id=1214782	A-MOZ-FIREF-310116/39
Denial of Service; Execute Code; Overflow; Memory Corruption	31-Jan-16	10	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 44.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to uninitialized memory encountered during brotli data compression, and other vectors. **Reference: CVE-2016-1931**	http://www.mozilla.org/security/announce/2016/mfsa2016-01.html	A-MOZ-FIREF-310116/40
Denial of Service; Overflow	31-Jan-16	10	The MoofParser::Metadata function in binding/MoofParser.cpp in libstagefright in Mozilla Firefox before 44.0 does not limit the size of read operations, which might allow remote attackers to cause a denial of service (integer overflow and buffer overflow) or possibly have unspecified other impact via crafted metadata. **Reference: CVE-2016-1946**	http://www.mozilla.org/security/announce/2016/mfsa2016-10.html	A-MOZ-FIREF-310116/41

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Denial of Service; Overflow	31-Jan-16	4.3	Integer overflow in the image-deinterlacing functionality in Mozilla Firefox before 44.0 allows remote attackers to cause a denial of service (memory consumption or application crash) via a crafted GIF image. **Reference: CVE-2016-1933**	http://www.mozilla.org/security/announce/2016/mfsa2016-02.html	A-MOZ-FIREF-310116/42
Denial of Service; Overflow; Memory Corruption	31-Jan-16	10	The Buffer11::NativeBuffer11::map function in ANGLE, as used in Mozilla Firefox before 44.0, might allow remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors. **Reference: CVE-2016-1944**	https://bugzilla.mozilla.org/show_bug.cgi?id=1186621	A-MOZ-FIREF-310116/43
Cross Site Scripting	31-Jan-16	4.3	The protocol-handler dialog in Mozilla Firefox before 44.0 allows remote attackers to conduct clickjacking attacks via a crafted web site that triggers a single-click action in a situation where a double-click action was intended. **Reference: CVE-2016-1937**	https://bugzilla.mozilla.org/show_bug.cgi?id=724353	A-MOZ-FIREF-310116/44
Not Available	31-Jan-16	4.3	Mozilla Firefox before 44.0 allows user-assisted remote attackers to spoof a trailing substring in the address bar by leveraging a user's paste of a (1) wyciwyg: URI or (2) resource: URI. **Reference: CVE-2016-1942**	https://bugzilla.mozilla.org/show_bug.cgi?id=1189082	A-MOZ-FIREF-310116/45
Not Available	31-Jan-16	4.3	Mozilla Firefox 43.x mishandles attempts to connect to the Application Reputation service, which makes it easier for remote attackers to trigger an unintended download by leveraging the absence of	https://bugzilla.mozilla.org/show_bug.cgi?id=1237103	A-MOZ-FIREF-310116/46

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			reputation data. **Reference: CVE-2016-1947**		
Firefox;Firefox Esr *Mozilla Firefox, a free Web browser. Firefox is created by a global non-profit dedicated to putting individuals in control online. ; Firefox ESR is intended for groups who deploy and maintain the desktop environment in large organizations such as schools, governments and businesses.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	31-Jan-16	10	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 44.0 and Firefox ESR 38.x before 38.6 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors. **Reference: CVE-2016-1930**	http://www.mozilla.org/security/announce/2016/mfsa2016-01.html	A-MOZ-FIREF-310116/47
Execute Code; Overflow	31-Jan-16	9.3	Buffer overflow in the BufferSubData function in Mozilla Firefox before 44.0 and Firefox ESR 38.x before 38.6 allows remote attackers to execute arbitrary code via crafted WebGL content. **Reference: CVE-2016-1935**	http://www.mozilla.org/security/announce/2016/mfsa2016-03.html	A-MOZ-FIREF-310116/48
Firefox;NSS *Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications.*					
Not Available	31-Jan-16	6.4	The s_mp_div function in lib/freebl/mpi/mpi.c in Mozilla Network Security Services (NSS) before 3.21, as used in Mozilla Firefox before 44.0, improperly divides numbers, which might make it easier for remote attackers to defeat cryptographic protection mechanisms by leveraging use of the (1) mp_div or (2) mp_exptmod function. **Reference: CVE-2016-1938**	http://www.mozilla.org/security/announce/2016/mfsa2016-07.html	A-MOZ-FIREF-310116/49
NEC					
Expresscluster X *NEC's award-winning ExpressCluster is a family of integrated high availability and*					

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
disaster recovery software providing fast recovery and continuous protection of Data					
Directory Traversal	30-Jan-16	7.8	Directory traversal vulnerability in WebManager in NEC EXPRESSCLUSTER X through 3.3 11.31 on Windows and through 3.3 3.3.1-1 on Linux and Solaris allows remote attackers to read arbitrary files via unspecified vectors. **Reference: CVE-2016-1145**	http://jpn.nec.com/security-info/secinfo/nv16-001.html	A-NEC-EXPRE-310116/50
NTP					
NTP					
Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers.					
Not Available	26-Jan-16	2.1	NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 do not verify peer associations of symmetric keys when authenticating packets, which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key, aka a "skeleton key." **Reference: CVE-2015-7974**	http://bugs.ntp.org/show_bug.cgi?id=2936	A-NTP-NTP-310116/51
Openjpeg					
Openjpeg					
Openjpeg is an open-source library to encode and decode JPEG 2000 images					
Denial of Service; Overflow	27-Jan-16	4.3	The opj_tgt_reset function in OpenJpeg 2016.1.18 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG 2000 image. **Reference: CVE-2016-1924**		A-OPE-OPENJ-310116/52
Denial of Service; Overflow	27-Jan-16	4.3	Heap-based buffer overflow in the opj_j2k_update_image_data function in OpenJpeg 2016.1.18 allows remote attackers to cause a denial of service (out-of-bounds read		A-OPE-OPENJ-310116/53

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			and application crash) via a crafted JPEG 2000 image. **Reference: CVE-2016-1923**		
Openstack					
Swift *Object Storage, is an open source object storage system that is licensed under the Apache 2.0 license and runs on standard server hardware. OpenStack Swift is best suited to backup and archive unstructured data, such as documents, images etc..*					
Denial of Service	29-Jan-16	5	OpenStack Object Storage (Swift) before 2.4.0 does not properly close client connections, which allows remote attackers to cause a denial of service (proxy-server resource consumption) via a series of interrupted requests to a Large Object URL. **Reference: CVE-2016-0737**	https://bugs.launchpad.net/swift/+bug/1466549	A-OPE-SWIFT-310116/54
Denial of Service	29-Jan-16	5	OpenStack Object Storage (Swift) before 2.3.1 (Kilo), 2.4.x, and 2.5.x before 2.5.1 (Liberty) do not properly close server connections, which allows remote attackers to cause a denial of service (proxy-server resource consumption) via a series of interrupted requests to a Large Object URL. **Reference: CVE-2016-0738**	https://bugs.launchpad.net/cloud-archive/+bug/1493303	A-OPE-SWIFT-310116/55
Privoxy					
Privoxy *Privoxy is a non-caching web proxy with filtering capabilities for enhancing privacy, manipulating cookies and modifying web page data*					
Denial of Service	27-Jan-16	5	The remove_chunked_transfer_coding function in filters.c in Privoxy before 3.0.24 allows remote attackers to cause a denial of service (invalid read and crash) via crafted chunk-encoded content. **Reference: CVE-2016-1982**	http://www.privoxy.org/announce.txt	A-PRI-PRIVO-310116/56
Denial of Service	27-Jan-16	5	The client_host function in parsers.c in Privoxy before	http://ijbswa.cvs.sourc	A-PRI-PRIVO-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			3.0.24 allows remote attackers to cause a denial of service (invalid read and crash) via an empty HTTP Host header. **Reference: CVE-2016-1983**	eforge.net/viewvc/ijbswa/current/parsers.c?r1=1.302&r2=1.303	310116/57
Roundcube					
Roundcube Webmail *Roundcube is a web-based IMAP email client. Roundcube's most prominent feature is the pervasive use of Ajax technology.*					
Directory Traversal	29-Jan-16	4	Absolute path traversal vulnerability in program/steps/addressbook/photo.inc in Roundcube before 1.0.6 and 1.1.x before 1.1.2 allows remote authenticated users to read arbitrary files via a full pathname in the _alt parameter, related to contact photo handling. **Reference: CVE-2015-8794**	http://trac.roundcube.net/changeset/6ccd4c54b/github	A-ROU-ROUND-310116/58
Execute Code; Directory Traversal	29-Jan-16	6	Directory traversal vulnerability in the set_skin function in program/include/rcmail_output_html.php in Roundcube before 1.0.8 and 1.1.x before 1.1.4 allows remote authenticated users with certain permissions to read arbitrary files or possibly execute arbitrary code via a .. (dot dot) in the _skin parameter to index.php. **Reference: CVE-2015-8770**	https://roundcube.net/news/2015/12/26/updates-1.1.4-and-1.0.8-released/	A-ROU-ROUND-310116/59
Cross Site Scripting	29-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in program/include/rcmail.php in Roundcube before 1.0.6 and 1.1.x before 1.1.2 allows remote attackers to inject arbitrary web script or HTML via the _mbox parameter in a mail task to the default URL, a different vulnerability than	https://roundcube.net/news/2015/06/05/updates-1.1.2-and-1.0.6-released/	A-ROU-ROUND-310116/60

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Reference: CVE-2011-2937. **Reference: CVE-2015-8793**		
Tuxfamily					
Chrony *A Unix-based NTP implementation specifically written to be suitable for computers with dial-up connections to the Internet.*					
Not Available	26-Jan-16	6.8	chrony before 1.31.2 and 2.x before 2.2.1 do not verify peer associations of symmetric keys when authenticating packets, which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key, aka a "skeleton key." **Reference: CVE-2016-1567**	http://chrony.tuxfamily.org/news.html#_20_jan_2016_chrony_2_2_1_and_chrony_1_31_2_released	A-TUX-CHRON-310116/61
Websquare					
Job Web System *This web system administrator sample job description can assist in your creating a job application that will attract job candidates who are qualified for the job.*					
Cross Site Scripting	30-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in JOB-CUBE -JOB WEB SYSTEM before 1.2.2 and -JOB WEB SYSTEM High Income 1.0.6 and earlier allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-1144**	http://www.ws-download.net/info.php?type=version&id=V0001081	A-WEB-JOB W-310116/62
Operating System(OS)					
Cisco					
300 Series Managed Switch Firmware *Cisco 300 Series Switches help small businesses create a more efficient, better-connected workforce.*					
Denial of Service	27-Jan-16	5	The web-management GUI implementation on Cisco Small Business SG300 devices 1.4.1.x allows remote attackers to cause a denial of service (HTTPS outage) via crafted HTTPS requests, aka Bug ID CSCuw87174. **Reference: CVE-2016-1299**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160127-sbms	O-CIS-300S-310116/63

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
500 Series Switch Firmware *Cisco 500 Series is a line of stackable managed switches that offer the advanced capabilities you need to support a more demanding network environment, at an affordable price*					
Denial of Service	30-Jan-16	7.8	The web GUI on Cisco Small Business 500 devices 1.2.0.92 allows remote attackers to cause a denial of service via a crafted HTTP request, aka Bug ID CSCul65330. **Reference: CVE-2016-1303**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160128-sbs	O-CIS-500S-310116/64
Rv Series Router Firmware *Cisco Small Business RV Series Routers provides small businesses (SMB) with highly secure VPN access, security with built-in firewalls, and simple installation.*					
Execute Code; Sql Injection	27-Jan-16	10	SQL injection vulnerability in the web-based management interface on Cisco RV220W devices allows remote attackers to execute arbitrary SQL commands via a crafted header in an HTTP request, aka Bug ID CSCuv29574. **Reference: CVE-2015-6319**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160127-rv220	O-CIS-RVSE-310116/65
Freebsd					
Freebsd *Freebsd is an operating system for a variety of platforms which focuses on features, speed, and stability.*					
Denial of Service	29-Jan-16	7.8	The Stream Control Transmission Protocol (SCTP) module in FreeBSD 9.3 before p33, 10.1 before p26, and 10.2 before p9, when the kernel is configured for IPv6, allows remote attackers to cause a denial of service (assertion failure or NULL pointer dereference and kernel panic) via a crafted ICMPv6 packet. **Reference: CVE-2016-1879**		O-FRE-FREEB-310116/66
Denial of Service	29-Jan-16	7.8	FreeBSD 9.3 before p33, 10.1 before p26, and 10.2 before p9 allow remote attackers to		O-FRE-FREEB-310116/6

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			cause a denial of service (kernel crash) via vectors related to creating a TCP connection with the TCP_MD5SIG and TCP_NOOPT socket options. **Reference: CVE-2016-1882**		7
Greenbone;Openvas					
Greenbone Os/Greenbone Security Assistant *The Greenbone OS (GOS) equips the Greenbone Security Manager appliances with a comprehensive and powerful basis.The main elements of Greenbone OS are the base operating system, a administrative interface and the scan applications.*					
Cross Site Scripting	26-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in the charts module in Greenbone Security Assistant (GSA) 6.x before 6.0.8 allows remote attackers to inject arbitrary web script or HTML via the aggregate_type parameter in a get_aggregate command to omp. **Reference: CVE-2016-1926**	http://www.greenbone.net/technology/gbsa2016-01.html	O-GRE-GREEN-310116/68
Siemens					
Ozw672 Firmware;Ozw772 Firmware *Web server OZW672 allows for remote plant control and monitoring via the web.*					
Cross Site Scripting	30-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in the login form in the integrated web server on Siemens OZW OZW672 devices before 6.00 and OZW772 devices before 6.00 allows remote attackers to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-1488**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-743465.pdf	O-SIE-OZW67-310116/69
Westermo					
Weos *Westermo is your premiere supplier of high quality, robust data communications equipment designed for harsh industrial applications.*					
Not Available	30-Jan-16	9.3	Westermo WeOS before 4.19.0 uses the same SSL private key across different customers' installations,	https://ics-cert.us-cert.gov/advisories/ICS	O-WES-WEOS-310116/70

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

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by leveraging knowledge of a key. **Reference: CVE-2015-7923**	A-16-028-01	

Operating System/Application (OS/A)

Matroska/Novell

Libmatroska/Leap;Opensuse

Libmatroska is a C++ library to parse Matroska files (.mkv and .mka). It depends on libebml to work.;openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.

Overflow; Gain Information	29-Jan-16	5	The KaxInternalBlock::ReadData function in libMatroska before 1.4.4 allows context-dependent attackers to obtain sensitive information from process heap memory via crafted EBML lacing, which triggers an invalid memory access. **Reference: CVE-2015-8792**	https://github.com/Matroska-Org/libmatroska/blob/release-1.4.4/ChangeLog	A-MAT-LIBMA-310116/71

Apple/Mozilla

Mac Os X/Firefox

OS X is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc.; Mozilla Firefox, a free Web browser. Firefox is created by a global non-profit dedicated to putting individuals in control online.

Cross Site Scripting	31-Jan-16	4.3	The file-download dialog in Mozilla Firefox before 44.0 on OS X enables a certain button too quickly, which allows remote attackers to conduct clickjacking attacks via a crafted web site that triggers a single-click action in a situation where a double-click action was intended. **Reference: CVE-2016-1941**	https://bugzilla.mozilla.org/show_bug.cgi?id=1116385	O-APP-MAC O-310116/72

Canonical;Debian/Haxx

Ubuntu Linux/Debian Linux/Curl

Ubuntu is a Debian-based Linux operating system and distribution for personal computers, smartphones and network servers. ;Curl is a computer software project

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
providing a library and command-line tool for transferring data using various protocol					
Not Available	29-Jan-16	5	The ConnectionExists function in lib/url.c in libcurl before 7.47.0 does not properly re-use NTLM-authenticated proxy connections, which might allow remote attackers to authenticate as other users via a request, a similar issue to CVE-2014-0015. **Reference: CVE-2016-0755**	http://curl.haxx.se/docs/adv_20160127A.html	O-CAN-UBUNT-310116/73
Google/Mozilla					
Android/Firefox					
Android is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices.; Mozilla Firefox, a free Web browser. Firefox is created by a global non-profit dedicated to putting individuals in control online.					
Not Available	31-Jan-16	4.3	Mozilla Firefox before 44.0 on Android does not ensure that HTTPS is used for a lightweight-theme installation, which allows man-in-the-middle attackers to replace a theme's images and colors by modifying the client-server data stream. **Reference: CVE-2016-1948**	https://bugzilla.mozilla.org/show_bug.cgi?id=1235876	O-GOO-ANDRO-310116/74
Not Available	31-Jan-16	4.3	Mozilla Firefox before 44.0 on Android allows remote attackers to spoof the address bar via the scrollTo method. **Reference: CVE-2016-1943**	https://bugzilla.mozilla.org/show_bug.cgi?id=1228590	O-GOO-ANDRO-310116/75
Not Available	31-Jan-16	5	Mozilla Firefox before 44.0 on Android allows remote attackers to spoof the address bar via a data: URL that is mishandled during (1) shortcut opening or (2) BOOKMARK intent processing. **Reference: CVE-2016-1940**	https://bugzilla.mozilla.org/show_bug.cgi?id=1208525	O-GOO-ANDRO-310116/76