National Critical Information Infrastructure Protection Centre

CVE Report

16 - 23 Jan 2016

Vol. 3 No.3

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Application (A)					
Cgit Project					
Cgit *Cgit is an attempt to create a fast web interface for the git version control system, using a built in cache to decrease pressure on the git server.*					
Overflow	20-Jan-16	7.5	Integer overflow in the authenticate_post function in CGit before 0.12 allows remote attackers to have unspecified impact via a large value in the Content-Length HTTP header, which triggers a buffer overflow. **Reference: CVE-2016-1901**	http://git.zx2c4.com/cgit/commit/?id=4458abf64172a62b92810c2293450106e6dfc763	A-CGI-CGIT-010216/1
Cross Site Scripting; Http R.Spl.	20-Jan-16	4.3	CRLF injection vulnerability in the cgit_print_http_headers function in ui-shared.c in CGit before 0.12 allows remote attackers with permission to write to a repository to inject arbitrary HTTP headers and conduct HTTP response splitting attacks or cross-site scripting (XSS) attacks via newline characters in a filename. **Reference: CVE-2016-1900**	http://git.zx2c4.com/cgit/commit/?id=513b3863d999f91b47d7e9f26710390db55f9463	A-CGI-CGIT-010216/2
Cross Site Scripting; Http R.Spl.	20-Jan-16	4.3	CRLF injection vulnerability in the ui-blob handler in CGit before 0.12 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks or cross-site scripting (XSS) attacks via CRLF sequences in the mimetype parameter, as demonstrated by a request to blob/cgit.c. **Reference: CVE-2016-1899**	http://git.zx2c4.com/cgit/commit/?id=1c581a072651524f3b0d91f33e22a42c4166dd96	A-CGI-CGIT-010216/3
Cisco					
Adaptive Security Appliance Software *Cisco ASA Software delivers enterprise-class security capabilities for the ASA security family in a variety of form factors.*					
Gain Information	16-Jan-16	5	Cisco Adaptive Security Appliance (ASA) Software 8.4 allows remote attackers to obtain sensitive information via an AnyConnect	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	A-CIS-ADAPT-010216/4

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			authentication attempt, aka Bug ID CSCuo65775. **Reference: CVE-2016-1295**	o-sa-20160115-asa	
Firesight System Software *Cisco FireSIGHT Management centrally manages network security and operational into physical and virtual hosts, operating systems, applications, services protocols.*					
Cross Site Scripting	16-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in the Management Center in Cisco FireSIGHT System Software 6.0.1 allows remote attackers to inject arbitrary web script or HTML via a crafted cookie, aka Bug ID CSCuw89094. **Reference: CVE-2016-1294**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160115-fmc1	A-CIS-FIRES-010216/5
Cross Site Scripting	16-Jan-16	4.3	Multiple cross-site scripting (XSS) vulnerabilities in the Management Center in Cisco FireSIGHT System Software 6.0.0 and 6.0.1 allow remote attackers to inject arbitrary web script or HTML via unspecified parameters, aka Bug ID CSCux40414. **Reference: CVE-2016-1293**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160115-FireSIGHT	A-CIS-FIRES-010216/6
Identity Services Engine Software *ISE is a policy management and control platform for wired, wireless, and VPN.*					
Bypass	23-Jan-16	6.8	Cisco Identity Services Engine (ISE) before 2.0 allows remote authenticated users to bypass intended web-resource access restrictions via a direct request, aka Bug ID CSCuu45926. **Reference: CVE-2015-6317**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160113-ise2	A-CIS-IDENT-010216/7
Web Security Appliance *Cisco Web Security Appliance provides exceptional web security and control for organizations of all sizes – integrated into one appliance.*					
Bypass	20-Jan-16	5	The proxy engine on Cisco Web Security Appliance (WSA) devices with software 8.5.3-055, 9.1.0-000, and 9.5.0-235 allows remote attackers to bypass intended proxy restrictions via a malformed HTTP method, aka Bug ID CSCux00848. **Reference: CVE-2016-1296**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160119-wsa	A-CIS-WEBS-010216/8
Ecryptfs					
Ecryptfs-utils *The enterprise cryptographic filesystem for Linux*					
Gain Privileges	22-Jan-16	4.6	mount.ecryptfs_private.c in eCryptfs-utils does not validate mount	https://bugs.launchpad.net/ecryptfs/	A-ECR-ECRYP-

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
			destination filesystem types, which allows local users to gain privileges by mounting over a nonstandard filesystem, as demonstrated by /proc/$pid. **Reference: CVE-2016-1572**	+bug/1530566	010216/9
GNU					
Glibc *The GNU C Library, commonly known as glibc, is the GNU Project's implementation of the C standard library*					
Bypass	20-Jan-16	2.1	The process_envvars function in elf/rtld.c in the GNU C Library (aka glibc or libc6) before 2.23 allows local users to bypass a pointer-guarding protection mechanism via a zero value of the LD_POINTER_GUARD environment variable. **Reference: CVE-2015-8777**	https://sourceware.org/bugzilla/show_bug.cgi?id=18928	A-GNU-GLIBC-010216/10
HP					
Arcsight Logger *HP ArcSight Logger is a borderless universal log management solution that can be deployed as an appliance, software, virtual machine, or within the cloud*					
Execute Code	16-Jan-16	6.5	HPE ArcSight Logger before 6.1P1 allows remote authenticated users to execute arbitrary code via unspecified input to the (1) Intellicus or (2) client-certificate upload component. **Reference: CVE-2015-6864**	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04941487	A-HP-ARCSI-010216/11
Execute Code	16-Jan-16	7.5	HPE ArcSight Logger before 6.1P1 allows remote attackers to execute arbitrary code via unspecified input to the (1) Intellicus or (2) client-certificate upload component. **Reference: CVE-2015-6863**		A-HP-ARCSI-010216/12
IBM					
Host On-demand *The IBM WebSphere Host On-Demand Server, or HOD as it is commonly known is a Java application that runs on a Server that is deliverable via modern web servers such as the Apache web server.*					
Cross Site Scripting	18-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in IBM Host On-Demand 11.0 through 11.0.14 allows remote attackers to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2015-5002**	http://www-01.ibm.com/support/docview.wss?uid=swg21973985	A-IBM-HOST - 010216/13
Infosphere Master Data Management *InfoSphere Master Data Management (MDM) is the most complete, proven and powerful MDM solution with*					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
collaborative and operational capabilities.					
Gain Information	17-Jan-16	2.1	IBM InfoSphere Master Data Management - Collaborative Edition 9.1, 10.1, 11.0 before 11.0.0.0 IF11, 11.3 before 11.3.0.0 IF7, and 11.4 before 11.4.0.4 IF1 does not properly restrict browser caching, which allows local users to obtain sensitive information by reading cache files. **Reference: CVE-2015-4958**	http://www-01.ibm.com/support/docview.wss?uid=swg21971545	A-IBM-INFOS-010216/14
Cross Site Scripting	17-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in the GDS component in IBM InfoSphere Master Data Management - Collaborative Edition 9.1, 10.1, 11.0 before 11.0.0.0 IF11, 11.3 before 11.3.0.0 IF7, and 11.4 before 11.4.0.4 IF1 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2015-7414**		A-IBM-INFOS-010216/15
Not Available	17-Jan-16	3.5	IBM InfoSphere Master Data Management - Collaborative Edition 9.1, 10.1, 11.0 before 11.0.0.0 IF11, 11.3 before 11.3.0.0 IF7, and 11.4 before 11.4.0.4 IF1 allows remote authenticated users to conduct clickjacking attacks via a crafted web site. **Reference: CVE-2015-4960**		A-IBM-INFOS-010216/16
Jazz Reporting Service *Jazz Reporting Service is an alternative to the complex reporting capabilities that are available in many Rational products and solutions. By including Jazz Reporting Service in your integrated lifecycle toolset, you can quickly and easily consolidate data from a variety of data sources across your tools and project areas.*					
Gain Information	17-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 man-in-the-middle attackers to obtain sensitive information via unspecified vectors, as demonstrated by login information. **Reference: CVE-2015-7470**	http://www-01.ibm.com/support/docview.wss?uid=swg21972485	A-IBM-JAZZ-010216/17
Bypass	17-Jan-16	4	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		A-IBM-JAZZ-010216/18

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			remote authenticated users to bypass intended read-only restrictions by leveraging a JazzGuest role. **Reference: CVE-2015-7469**		
Bypass	17-Jan-16	4	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 authenticated users to bypass intended restrictions on administrator tasks via unspecified vectors. **Reference: CVE-2015-7468**		A-IBM-JAZZ-010216/19
Cross Site Scripting	17-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in 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 authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2015-7467**		A-IBM-JAZZ-010216/20
Tealeaf Customer Experience *IBM Tealeaf CX improves the online customer experience by capturing and managing visitor interactions on website*					
Directory Traversal	18-Jan-16	7.8	Directory traversal vulnerability in the replay server in IBM Tealeaf Customer Experience before 8.7.1.8818, 8.8 before 8.8.0.9026, 9.0.0, 9.0.0A, 9.0.1 before 9.0.1.1083, 9.0.1A before 9.0.1.5073, 9.0.2 before 9.0.2.1095, and 9.0.2A before 9.0.2.5144 allows remote attackers to read arbitrary files via unspecified vectors. **Reference: CVE-2015-4988**	http://www-01.ibm.com/support/docview.wss?uid=swg21968868	A-IBM-TEALE-010216/21
Tivoli Federated Identity Manager *IBM Tivoli Federated Identity Manager Business Gateway enables users inside and outside of your organization to securely sign on to disparate networks*					
Cross Site Scripting	18-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in IBM Tivoli Federated Identity Manager (TFIM) 6.2.2 before FP16 allows remote attackers to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2015-4959**	http://www-01.ibm.com/support/docview.wss?uid=swg21974157	A-IBM-TIVOL-010216/22
Tivoli Storage Manager					

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
IBM Spectrum Protect (Tivoli Storage Manager) is a data protection platform that gives enterprises a single point of control and administration for backup and recovery					
Denial of Service	20-Jan-16	5	Client Acceptor Daemon (CAD) in the client in IBM Spectrum Protect (formerly Tivoli Storage Manager) 5.5 and 6.x before 6.3.2.5, 6.4 before 6.4.3.1, and 7.1 before 7.1.3 allows remote attackers to cause a denial of service (daemon crash) via a crafted Web client URL. **Reference: CVE-2015-4951**	http://www-01.ibm.com/support/docview.wss?uid=swg21973484	A-IBM-TIVOL-010216/23
Websphere Application Server *WebSphere Application Server (WAS) is a software product that performs the role of a web application server. More specifically, it is a software framework and middleware that hosts Java based web applications.*					
Cross Site Scripting	23-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in IBM WebSphere Application Server 7.0 before 7.0.0.41, 8.0 before 8.0.0.12, and 8.5 before 8.5.5.9 allows remote authenticated users to inject arbitrary web script or HTML via crafted data from an OAuth provider. **Reference: CVE-2015-7417**	http://www-01.ibm.com/support/docview.wss?uid=swg21974520	A-IBM-WEBSP-010216/24
Websphere Commerce *IBM WebSphere Commerce AKA WCS (WebSphere Commerce Suite) is a software platform framework for e-commerce, including marketing, sales, customer and order processing functionality in a tailorable, integrated package.*					
Cross Site Scripting	18-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in IBM WebSphere Commerce 6.0 through FP11, 6.0 Feature Pack 4, 7.0 through FP9, 7.0 Feature Pack 5 through 8, and 8.0 before 8.0.0.1 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2015-5009**	http://www-01.ibm.com/support/docview.wss?uid=swg21972610	A-IBM-WEBSP-010216/25
Cross Site Scripting	18-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in IBM WebSphere Commerce 6.0 through FP11, 6.0 Feature Pack 4, 7.0 through FP9, 7.0 Feature Pack 5 through 8, and 8.0 before 8.0.0.1 allows remote attackers to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2015-5008**		A-IBM-WEBSP-010216/26
Websphere Mq Light *IBM MQ Light simplifies incorporating asynchronous messaging into applications and deploying them into*					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
larger MQ-based infrastructures.					
Denial of Service	18-Jan-16	5	IBM WebSphere MQ Light 1.x before 1.0.2 allows remote attackers to cause a denial of service (MQXR service crash) via a series of connect and disconnect actions. **Reference: CVE-2015-4942**	http://www-01.ibm.com/support/docview.wss?uid=swg21974169	A-IBM-WEBSP-010216/27
ISC					
Bind *BIND is the most widely used Domain Name System (DNS) software on the Internet. On Unix-like operating systems it is the de facto standard*					
Denial of Service	20-Jan-16	6.6	buffer.c in named in ISC BIND 9.10.x before 9.10.3-P3, when debug logging is enabled, allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit, or daemon crash) or possibly have unspecified other impact via (1) OPT data or (2) an ECS option. **Reference: CVE-2015-8705**	https://kb.isc.org/article/AA-01336	A-ISC-BIND-010216/28
Denial of Service	20-Jan-16	6.8	apl_42.c in ISC BIND 9.x before 9.9.8-P3 and 9.9.x and 9.10.x before 9.10.3-P3 allows remote authenticated users to cause a denial of service (INSIST assertion failure and daemon exit) via a malformed Address Prefix List (APL) record. **Reference: CVE-2015-8704**	https://kb.isc.org/article/AA-01335	A-ISC-BIND-010216/29
Jasper Project					
Jasper *Jasper is an open source platform for developing always-on, voice-controlled applications.*					
Denial of Service; Overflow	20-Jan-16	4.3	The jpc_pi_nextcprl function in JasPer 1.900.1 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG 2000 image. **Reference: CVE-2016-1867**	http://www.openwall.com/lists/oss-security/2016/01/13/2	A-JAS-JASPE-010216/30
Libpng					
Libpng *libpng is the official Portable Network Graphics (PNG) reference library (originally called pnglib).*					
Denial of Service; Overflow	21-Jan-16	7.5	Buffer overflow in the png_set_PLTE function in libpng before 1.0.65, 1.1.x and 1.2.x before 1.2.55, 1.3.x, 1.4.x before 1.4.18, 1.5.x before 1.5.25, and 1.6.x before 1.6.20 allows	http://sourceforge.net/projects/libpng/files/libpng10/1.0.65/	A-LIB-LIBPN-010216/31

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a small bit-depth value in an IHDR (aka image header) chunk in a PNG image. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-8126. **Reference: CVE-2015-8472**		
Openbsd					
Openssh *OpenSSH, also known as OpenBSD Secure Shell, is a suite of security-related network-level utilities based on the SSH protocol, which help to secure network*					
Denial of Service; Overflow	19-Jan-16	5	The ssh_packet_read_poll2 function in packet.c in OpenSSH before 7.1p2 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via crafted network traffic. **Reference: CVE-2016-1907**	https://anongit.mindrot.org/openssh.git/commit/?id=2fecfd486bdba9f51b3a789277bb0733ca36e1c0	A-OPE-OPENS-010216/32
Openstack					
Heat *Heat is the main project in the OpenStack Orchestration program. It implements an orchestration engine to launch multiple composite cloud applications by executing appropriate OpenStack API calls to generate running cloud.*					
Denial of Service; Overflow	20-Jan-16	5.5	The template-validate command in OpenStack Orchestration API (Heat) before 2015.1.3 (kilo) and 5.0.x before 5.0.1 (liberty) allows remote authenticated users to cause a denial of service (memory consumption) or determine the existence of local files via the resource type in a template, as demonstrated by file:///dev/zero. **Reference: CVE-2015-5295**	https://security.openstack.org/ossa/OSSA-2016-003.html	A-OPE-HEAT-010216/33
PHP					
PHP *PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language.*					
Directory Traversal	19-Jan-16	5	Directory traversal vulnerability in the PharData class in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to write to arbitrary files via a .. (dot dot) in a ZIP archive entry that is mishandled during an extractTo call.	http://www.php.net/ChangeLog-5.php	A-PHP-PHP-010216/34

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-2015-6833		
Denial of Service	19-Jan-16	7.5	Use-after-free vulnerability in the Collator::sortWithSortKeys function in ext/intl/collator/collator_sort.c in PHP 7.x before 7.0.1 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging the relationships between a key buffer and a destroyed array. **Reference: CVE-2015-8616**	https://bugs.php.net/bug.php?id=71020	A-PHP-PHP-010216/35
Denial of Service; Overflow	19-Jan-16	7.5	Multiple integer overflows in ext/standard/exec.c in PHP 7.x before 7.0.2 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a long string to the (1) php_escape_shell_cmd or (2) php_escape_shell_arg function, leading to a heap-based buffer overflow. **Reference: CVE-2016-1904**	https://github.com/php/php-src/commit/2871c70efaaaa0f102557a17c727fd4d5204dd4b	A-PHP-PHP-010216/36
Denial of Service; Overflow	19-Jan-16	7.5	Stack-based buffer overflow in the phar_fix_filepath function in ext/phar/phar.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large length value, as demonstrated by mishandling of an e-mail attachment by the imap PHP extension. **Reference: CVE-2015-5590**	https://bugs.php.net/bug.php?id=69923	A-PHP-PHP-010216/37
Denial of Service; Overflow; Gain Information	19-Jan-16	6.4	The gdImageRotateInterpolated function in ext/gd/libgd/gd_interpolation.c in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a large bgd_color argument to the imagerotate function. **Reference: CVE-2016-1903**	http://www.php.net/ChangeLog-5.php	A-PHP-PHP-010216/38
Execute Code	19-Jan-16	10	Format string vulnerability in the	http://php.net/Ch	A-PHP-

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
			zend_throw_or_error function in Zend/zend_execute_API.c in PHP 7.x before 7.0.1 allows remote attackers to execute arbitrary code via format string specifiers in a string that is misused as a class name, leading to incorrect error handling. **Reference: CVE-2015-8617**	angeLog-7.php	PHP-010216/39
Execute Code	19-Jan-16	7.5	The SoapClient __call method in ext/soap/soap.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 does not properly manage headers, which allows remote attackers to execute arbitrary code via crafted serialized data that triggers a "type confusion" in the serialize_function_call function. **Reference: CVE-2015-6836**	https://bugs.php.net/bug.php?id=70388	A-PHP-PHP-010216/40
Execute Code	19-Jan-16	7.5	Use-after-free vulnerability in the SPL unserialize implementation in ext/spl/spl_array.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to execute arbitrary code via crafted serialized data that triggers misuse of an array field. **Reference: CVE-2015-6832**	https://bugs.php.net/bug.php?id=70068	A-PHP-PHP-010216/41
Execute Code	19-Jan-16	7.5	Multiple use-after-free vulnerabilities in SPL in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allow remote attackers to execute arbitrary code via vectors involving (1) ArrayObject, (2) SplObjectStorage, and (3) SplDoublyLinkedList, which are mishandled during unserialization. **Reference: CVE-2015-6831**	http://www.php.net/ChangeLog-5.php	A-PHP-PHP-010216/42
Execute Code	19-Jan-16	7.5	The php_str_replace_in_subject function in ext/standard/string.c in PHP 7.x before 7.0.0 allows remote attackers to execute arbitrary code via a crafted value in the third argument to the str_ireplace function. **Reference: CVE-2015-6527**	https://bugs.php.net/bug.php?id=70140	A-PHP-PHP-010216/43
SAP					
Hana					

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
SAP HANA is an application server that includes an in-memory, column-oriented, relational database management system.					
Denial of Service	20-Jan-16	8.5	The XS engine in SAP HANA allows remote attackers to spoof log entries in trace files and consequently cause a denial of service (disk consumption and process crash) via a crafted HTTP request, related to an unspecified debug function, aka SAP Security Note 2241978. **Reference: CVE-2016-1929**	http://erpscan.com/press-center/blog/sap-security-notes-january-2016-review/	A-SAP-HANA-010216/44
Denial of Service; Execute Code; Overflow	20-Jan-16	7.5	Buffer overflow in the XS engine (hdbxsengine) in SAP HANA allows remote attackers to cause a denial of service or execute arbitrary code via a crafted HTTP request, related to JSON, aka SAP Security Note 2241978. **Reference: CVE-2016-1928**		A-SAP-HANA-010216/45
Wolfssl					
Wolfssl *wolfSSL offers an embedded SSL implementation that is portable, progressive, and easy to use with products including the wolfSSL embedded SSL library*					
Denial of Service	22-Jan-16	5	wolfSSL (formerly CyaSSL) before 3.6.8 allows remote attackers to cause a denial of service (resource consumption or traffic amplification) via a crafted DTLS cookie in a ClientHello message. **Reference: CVE-2015-6925**	http://wolfssl.com/wolfSSL/Docs-wolfssl-changelog.html	A-WOL-WOLFS-010216/46
Not Available	22-Jan-16	2.6	wolfSSL (formerly CyaSSL) before 3.6.8 does not properly handle faults associated with the Chinese Remainder Theorm (CRT) process when allowing ephemeral key exchange without low memory optimizations on a server, which makes it easier for remote attackers to obtain private RSA keys by capturing TLS handshakes, aka a Lenstra attack. **Reference: CVE-2015-7744**	https://wolfssl.com/wolfSSL/Blog/Entries/2015/9/17_Two_Vulnerabilities_Recently_Found%2C_An_Attack_on_RSA_using_CRT_and_DoS_Vulnerability_With_DTLS.html	A-WOL-WOLFS-010216/47
Application/Hardware (A/H)					
F5/F5					
Big-ip Access Policy Manager;Big-ip Advanced Firewall Manager;Big-ip Analytics;Big-ip Application Acceleration Manager;Big-ip Application Security Manager;Big-ip Edge Gateway;Big-ip Enterprise Manager;Big-ip Global Traffic Manager;Big-ip Link Controller;Big-ip Local Traffic Manager;Big-ip Policy Enforcement Manager;Big-ip Wan Optimization Manager;Big-ip Webaccelerator;Big-iq					

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
Application Delivery Controller;Big-iq Cloud;Big-iq Device;Big-iq Security/Big-ip Protocol Security Manager *NR*					
Denial of Service	20-Jan-16	7.8	Memory leak in the last hop kernel module in F5 BIG-IP LTM, GTM, and Link Controller 10.1.x, 10.2.x before 10.2.4 HF13, 11.x before 11.2.1 HF15, 11.3.x, 11.4.x, 11.5.x before 11.5.3 HF2, and 11.6.x before HF6, BIG-IP AAM 11.4.x, 11.5.x before 11.5.3 HF2 and 11.6.0 before HF6, BIG-IP AFM and PEM 11.3.x, 11.4.x, 11.5.x before 11.5.3 HF2, and 11.6.0 before HF6, BIG-IP Analytics 11.x before 11.2.1 HF15, 11.3.x, 11.4.x, 11.5.x before 11.5.3 HF2, and 11.6.0 before HF6, BIG-IP APM and ASM 10.1.0 through 10.2.4, 11.x before 11.2.1 HF15, 11.3.x, 11.4.x, 11.5.x before 11.5.3 HF2, and 11.6.0 before HF6, BIG-IP Edge Gateway, WebAccelerator, and WOM 10.1.x, 10.2.x before 10.2.4 HF13, 11.x before 11.2.1 HF15, and 11.3.0, BIG-IP PSM 10.1.x, 10.2.x before 10.2.4 HF13, 11.x before 11.2.1 HF15, 11.3.x, and 11.4.x before 11.4.1 HF, Enterprise Manager 3.0.0 through 3.1.1, BIG-IQ Cloud and Security 4.0.0 through 4.5.0, BIG-IQ Device 4.2.0 through 4.5.0, and BIG-IQ ADC 4.5.0 might allow remote attackers to cause a denial of service (memory consumption) via a large number of crafted UDP packets. **Reference: CVE-2015-5516**	https://support.f5.com/kb/en-us/solutions/public/k/00/sol00032124.html	A-H-F5/-BIG-I-010216/48
Operating System (OS)					
Cisco					
Modular Encoding Platform D9036 Software *Cisco Modular Encoding Platform D9036 provides multi-resolution, multi-format encoding for applications requiring high levels of video quality.*					
Not Available	22-Jan-16	10	Cisco Modular Encoding Platform D9036 Software before 02.04.70 has hardcoded (1) root and (2) guest passwords, which makes it easier for remote attackers to obtain access via an SSH session, aka Bug ID CSCut88070.	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160120-d9036	OS-CIS-MODUL-010216/49

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-2015-6412		
Harman					
Amx Firmware *AMX firmware solves the complexity of managing technology with reliable, consistent and scalable systems comprising control and automation, system-wide switching and AV signal distribution, digital signage and technology management.*					
Not Available	22-Jan-16	10	The setUpSubtleUserAccount function in /bin/bw on Harman AMX devices before 2016-01-20 has a hardcoded password for the 1MB@tMaN account, which makes it easier for remote attackers to obtain access via a (1) SSH or (2) HTTP session, a different vulnerability than CVE-2015-8362. **Reference: CVE-2016-1984**	http://www.amx.com/techcenter/firmware.asp?Category=Hot%20Fix%20Files	OS-HAR-AMX F-010216/50
Not Available	22-Jan-16	10	The setUpSubtleUserAccount function in /bin/bw on Harman AMX devices before 2015-10-12 has a hardcoded password for the BlackWidow account, which makes it easier for remote attackers to obtain access via a (1) SSH or (2) HTTP session, a different vulnerability than CVE-2016-1984. **Reference: CVE-2015-8362**	http://www.amx.com/techcenter/NXSecurityBrief/	OS-HAR-AMX F-010216/51
IBM					
Security Network Protection Firmware *IBM Security Network Protection is a firmware for the XGS NGIPS network protection platform.*					
Gain Information	18-Jan-16	4.3	GSKit in IBM Security Network Protection 5.3.1 before 5.3.1.7 and 5.3.2 allows remote attackers to discover credentials by triggering an MD5 collision. **Reference: CVE-2016-0201**	http://www-01.ibm.com/support/docview.wss?uid=swg21974242	OS-IBM-SECUR-010216/52
Netapp					
ONTAP *The Data ONTAP operating system implements a single proprietary file-system called WAFL. When used for file storage, Data ONTAP is capable of acting as both a NFS server and/or a CIFS server, contingent on licensing and configuration.*					
Gain Information	18-Jan-16	4.3	NetApp Data ONTAP before 8.2.4P1, when 7-Mode and HTTP access are enabled, allows remote attackers to obtain sensitive volume information via unspecified vectors. **Reference: CVE-2015-7886**	http://kb.netapp.com/support/index?page=content&id=9010055	OS-NET-ONTAP-010216/53
Operating System/Application (OS/A)					

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
Cisco					
Firepower Extensible Operating System/Unified Computing System *The Cisco Firepower security appliance is a next-generation platform for network and content security solutions.; The Cisco Unified Computing System (UCS) is an (x86) architecture data center server platform composed of computing hardware, virtualization support, switching fabric, and management software introduced in 2009*					
Execute Code	22-Jan-16	10	An unspecified CGI script in Cisco FX-OS before 1.1.2 on Firepower 9000 devices and Cisco Unified Computing System (UCS) Manager before 2.2(4b), 2.2(5) before 2.2(5a), and 3.0 before 3.0(2e) allows remote attackers to execute arbitrary shell commands via a crafted HTTP request, aka Bug ID CSCur90888. **Reference: CVE-2015-6435**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160120-ucsm	OS-A-CIS-FIREP-010216/54
XEN					
XEN *Xen Project is a hypervisor using a microkernel design, providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently.*					
Denial of Service	22-Jan-16	4.7	The paging_invlpg function in include/asm-x86/paging.h in Xen 3.3.x through 4.6.x, when using shadow mode paging or nested virtualization is enabled, allows local HVM guest users to cause a denial of service (host crash) via a non-canonical guest address in an INVVPID instruction, which triggers a hypervisor bug check. **Reference: CVE-2016-1571**	http://xenbits.xen.org/xsa/advisory-168.html	OS-A-XEN-XEN - 010216/55
Denial of Service; Gain Privileges; Gain Information	22-Jan-16	6.9	The PV superpage functionality in arch/x86/mm.c in Xen 3.4.0, 3.4.1, and 4.1.x through 4.6.x allows local PV guests to obtain sensitive information, cause a denial of service, gain privileges, or have unspecified other impact via a crafted page identifier (MFN) to the (1) MMUEXT_MARK_SUPER or (2) MMUEXT_UNMARK_SUPER sub-op in the HYPERVISOR_mmuext_op hypercall or (3) unknown vectors related to page table updates. **Reference: CVE-2016-1570**	http://xenbits.xen.org/xsa/advisory-167.html	OS-A-XEN-XEN - 010216/56