Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Application (A)					
Acquia					
Mollom *Mollom is a free web service to get rid of spam, unwanted content and fake users on your Drupal, Wordpress and Joomla site or blog.*					
Bypass	08-Jan-16	5	The Mollom module 6.x-2.7 before 6.x-2.15 for Drupal allows remote attackers to bypass intended access restrictions and modify the mollom blacklist via unspecified vectors. **Reference: CVE-2015-8754**	https://www.drupal.org/node/2626872	A-ACQ-MOLLO-220116/1
Adobe					
Acrobat;Acrobat Dc;Acrobat Reader;Acrobat Reader Dc *Adobe Acrobat Reader DC software is the free global standard for reliably viewing, printing, and commenting on PDF documents.*					
Bypass	14-Jan-16	6.8	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X mishandle the Global object, which allows attackers to bypass JavaScript API execution restrictions via unspecified vectors. **Reference: CVE-2016-0943**	https://helpx.adobe.com/security/products/acrobat/apsb16-02.html	A-ADO-ACROB-220116/2
Denial of Service; Execute Code; Overflow; Memory Corruption	14-Jan-16	6.8	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (uninitialized pointer dereference and memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946. **Reference: CVE-2016-0939**		A-ADO-ACROB-220116/3
Denial of Service; Execute Code; Overflow; Memory	14-Jan-16	6.8	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on		A-ADO-ACROB-220116/4

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Corruption			Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted FileAttachment annotation, a different vulnerability than CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946. **Reference: CVE-2016-0931**		
Execute Code	14-Jan-16	6.8	Use-after-free vulnerability in the Search object implementation in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0932, CVE-2016-0934, CVE-2016-0937, and CVE-2016-0940. **Reference: CVE-2016-0941**		A-ADO-ACROB-220116/5
Execute Code	14-Jan-16	6.8	Double free vulnerability in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via a crafted ExtGState dictionary. ***Reference: CVE-2016-0935***		A-ADO-ACROB-220116/6
Execute Code	14-Jan-16	6.8	Use-after-free vulnerability in AGM.dll in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via a multiple-layer PDF document, a different vulnerability than CVE-2016-0932, CVE-2016-0937, CVE-2016-0940, and CVE-2016-0941. ***Reference: CVE-2016-0934***		A-ADO-ACROB-220116/7
Execute Code	14-Jan-16	6.8	Use-after-free vulnerability in the Doc object implementation in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before		A-ADO-ACROB-220116/8

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0934, CVE-2016-0937, CVE-2016-0940, and CVE-2016-0941. ***Reference: CVE-2016-0932***		
Gain Privileges	14-Jan-16	7.2	Untrusted search path vulnerability in Adobe Download Manager, as used in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X, allows local users to gain privileges via a crafted resource in an unspecified directory. ***Reference: CVE-2016-0947***		A-ADO-ACROB-220116/9
Denial of Service; Execute Code; Overflow; Memory Corruption	14-Jan-16	9.3	The AcroForm plugin in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946. ***Reference: CVE-2016-0938***		A-ADO-ACROB-220116/10
Denial of Service; Execute Code; Overflow; Memory Corruption	14-Jan-16	9.3	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted JPEG 2000 data, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946. ***Reference: CVE-2016-0936***		A-ADO-ACROB-220116/11
Execute Code	14-Jan-16	9.3	Use-after-free vulnerability in the OCG object implementation in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before		A-ADO-ACROB-220116/12

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0932, CVE-2016-0934, CVE-2016-0940, and CVE-2016-0941. ***Reference: CVE-2016-0937***		
Denial of Service; Execute Code; Overflow; Memory Corruption	14-Jan-16	9.3	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, and CVE-2016-0945. ***Reference: CVE-2016-0946***		A-ADO-ACROB-220116/13
Denial of Service; Execute Code; Overflow; Memory Corruption	14-Jan-16	9.3	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, and CVE-2016-0946. ***Reference: CVE-2016-0945***		A-ADO-ACROB-220116/14
Denial of Service; Execute Code; Overflow; Memory Corruption	14-Jan-16	9.3	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0945, and CVE-2016-0946. ***Reference: CVE-2016-0944***		A-ADO-ACROB-220116/15

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; Execute Code; Overflow; Memory Corruption	14-Jan-16	9.3	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946. ***Reference: CVE-2016-0942***		A-ADO-ACROB-220116/16
Denial of Service; Execute Code; Overflow; Memory Corruption	14-Jan-16	9.3	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0931, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946. ***Reference: CVE-2016-0933***		A-ADO-ACROB-220116/17
Execute Code	14-Jan-16	9.3	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.30119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0932, CVE-2016-0934, CVE-2016-0937, and CVE-2016-0941. ***Reference: CVE-2016-0940***		A-ADO-ACROB-220116/18
Advantech					
Webaccess *Web Access is an enterprise business solutions provider for SMEs and an open source solutions provider for non-profits.*					
Cross-site Request Forgery	14-Jan-16	6.8	Cross-site request forgery (CSRF) vulnerability in Advantech WebAccess before 8.1 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors. ***Reference: CVE-2015-3946***	https://ics-cert.us-cert.gov/advisories/ICSA-16-014-01	A-ADV-WEBAC-220116/19
Denial of	14-Jan-16	7.8	Advantech WebAccess before 8.1 allows		A-ADV-

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
Service			remote attackers to cause a denial of service (out-of-bounds memory access) via unspecified vectors. ***Reference: CVE-2016-0851***		WEBAC-220116/20
Execute Code	14-Jan-16	10	Advantech WebAccess before 8.1 allows remote attackers to execute arbitrary code via vectors involving a browser plugin. ***Reference: CVE-2015-6467***		A-ADV-WEBAC-220116/21
Execute Code; Sql Injection	14-Jan-16	6.8	SQL injection vulnerability in Advantech WebAccess before 8.1 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors. ***Reference: CVE-2015-3947***		A-ADV-WEBAC-220116/22
Cross Site Scripting	14-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in Advantech WebAccess before 8.1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. ***Reference: CVE-2015-3948***		A-ADV-WEBAC-220116/23
Not Available	14-Jan-16	5	Advantech WebAccess before 8.1 allows remote attackers to read sensitive cleartext information about e-mail project accounts via unspecified vectors. ***Reference: CVE-2015-3943***		A-ADV-WEBAC-220116/24
Apache					
Subversion *Apache Subversion (often abbreviated SVN, after the command name svn) is a software versioning and revision control system distributed as free software under the Apache License.*					
Execute Code; Overflow	08-Jan-16	9	Integer overflow in the read_string function in libsvn_ra_svn/marshal.c in Apache Subversion 1.9.x before 1.9.3 allows remote attackers to execute arbitrary code via an svn:// protocol string, which triggers a heap-based buffer overflow and an out-of-bounds read. ***Reference: CVE-2015-5259***	http://subversion.apache.org/security/CVE-2015-5259-advisory.txt	A-APA-SUBVE-220116/25
Apple					
Quicktime *QuickTime is an extensible multimedia framework developed by Apple Inc., capable of handling various formats of digital video, picture, sound, panoramic images, and interactivity.*					
Denial of Service; Execute Code; Overflow	08-Jan-16	6.8	Apple QuickTime before 7.7.9 allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow and application crash) via a crafted TXXX frame within an ID3 tag in MP3 data in a movie file, a different vulnerability than CVE-2015-7085, CVE-2015-7086, CVE-2015-7087, CVE-2015-7088, CVE-2015-7089, CVE-	https://support.apple.com/HT205638	A-APP-QUICK-220116/26

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
			2015-7090, CVE-2015-7091, and CVE-2015-7117. ***Reference: CVE-2015-7092***		
Denial of Service; Execute Code; Overflow; Memory Corruption	08-Jan-16	6.8	Apple QuickTime before 7.7.9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted movie file, a different vulnerability than CVE-2015-7085, CVE-2015-7086, CVE-2015-7087, CVE-2015-7088, CVE-2015-7089, CVE-2015-7090, CVE-2015-7091, and CVE-2015-7092. ***Reference: CVE-2015-7117***		A-APP-QUICK-220116/27
Denial of Service; Execute Code; Overflow; Memory Corruption	08-Jan-16	6.8	Apple QuickTime before 7.7.9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted movie file, a different vulnerability than CVE-2015-7085, CVE-2015-7086, CVE-2015-7087, CVE-2015-7088, CVE-2015-7089, CVE-2015-7090, CVE-2015-7092, and CVE-2015-7117. ***Reference: CVE-2015-7091***		A-APP-QUICK-220116/28
Denial of Service; Execute Code; Overflow; Memory Corruption	08-Jan-16	6.8	Apple QuickTime before 7.7.9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted movie file, a different vulnerability than CVE-2015-7085, CVE-2015-7086, CVE-2015-7087, CVE-2015-7088, CVE-2015-7089, CVE-2015-7091, CVE-2015-7092, and CVE-2015-7117. ***Reference: CVE-2015-7090***		A-APP-QUICK-220116/29
Denial of Service; Execute Code; Overflow; Memory Corruption	08-Jan-16	6.8	Apple QuickTime before 7.7.9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted movie file, a different vulnerability than CVE-2015-7085, CVE-2015-7086, CVE-2015-7087, CVE-2015-7088, CVE-2015-7090, CVE-2015-7091, CVE-2015-7092, and CVE-2015-7117. ***Reference: CVE-2015-7089***		A-APP-QUICK-220116/30
Denial of Service; Execute Code; Overflow; Memory Corruption	08-Jan-16	6.8	Apple QuickTime before 7.7.9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted movie file, a different vulnerability than CVE-2015-7085, CVE-2015-7086, CVE-2015-7087, CVE-2015-7089, CVE-2015-7090, CVE-2015-7091,		A-APP-QUICK-220116/31

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			CVE-2015-7092, and CVE-2015-7117. ***Reference: CVE-2015-7088***		
Denial of Service; Execute Code; Overflow; Memory Corruption	08-Jan-16	6.8	Apple QuickTime before 7.7.9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted movie file, a different vulnerability than CVE-2015-7085, CVE-2015-7086, CVE-2015-7088, CVE-2015-7089, CVE-2015-7090, CVE-2015-7091, CVE-2015-7092, and CVE-2015-7117. ***Reference: CVE-2015-7087***		A-APP-QUICK-220116/32
Denial of Service; Execute Code; Overflow; Memory Corruption	08-Jan-16	6.8	Apple QuickTime before 7.7.9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted movie file, a different vulnerability than CVE-2015-7085, CVE-2015-7087, CVE-2015-7088, CVE-2015-7089, CVE-2015-7090, CVE-2015-7091, CVE-2015-7092, and CVE-2015-7117. ***Reference: CVE-2015-7086***		A-APP-QUICK-220116/33
Denial of Service; Execute Code; Overflow; Memory Corruption	08-Jan-16	6.8	Apple QuickTime before 7.7.9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted movie file, a different vulnerability than CVE-2015-7086, CVE-2015-7087, CVE-2015-7088, CVE-2015-7089, CVE-2015-7090, CVE-2015-7091, CVE-2015-7092, and CVE-2015-7117. ***Reference: CVE-2015-7085***		A-APP-QUICK-220116/34
Atlassian					
Jira;Jira Core;Jira Service Desk *JIRA Software offers flexible issue and project tracking with best-in-class agile tooling for software teams.;* *JIRA Core is a JIRA application that provides you with a workflow management system that you can use for many things, including running projects, tracking.;* *JIRA Service Desk combines the productivity and power of the JIRA platform with an intuitive user experience that allows service teams to focus on the customer.*					
Gain Information	08-Jan-16	3.5	Atlassian JIRA Software 7.0.3, JIRA Core 7.0.3, and the bundled JIRA Service Desk 3.0.3 installer attaches the wrong image to e-mail notifications when a user views an issue with inline wiki markup referencing an image attachment, which might allow remote attackers to obtain sensitive information by updating a different issue that includes wiki markup for an external image reference. ***Reference: CVE-2015-8481***	https://jira.atlassian.com/browse/JRA-47557	A-ATL-JIRA-220116/35
Bluecoat					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Advanced Secure Gateway; Proxysg *The Advanced Secure Gateway (ASG) is a new Secure Web Gateway from Blue Coat.* *ProxySG appliances are part of the Unified Security solution, and provide complete control over all your web traffic—with robust features that include user*					
Not Available	08-Jan-16	5.8	Open redirect vulnerability in Blue Coat ProxySG 6.5 before 6.5.8.8 and 6.6 and Advanced Secure Gateway (ASG) 6.6 might allow remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a base64-encoded URL in conjunction with a "clear text" one in a coaching page, as demonstrated by "http://www.%humbug-URL%.local/bluecoat-splash-API?%BASE64-URL%." ***Reference: CVE-2015-8597***	https://bto.bluecoat.com/security-advisory/sa107	A-BLU-ADVAN-220116/36
Blueman Project					
Blueman *Blueman is a bluetooth management utility using bluez dbus backend. It is designed to be easy to use for most common bluetooth tasks*					
Gain Privileges	08-Jan-16	7.2	The EnableNetwork method in the Network class in plugins/mechanism/Network.py in Blueman before 2.0.3 allows local users to gain privileges via the dhcp_handler argument. ***Reference: CVE-2015-8612***	https://github.com/blueman-project/blueman/issues/416	A-BLU-BLUEM-220116/37
Cisco					
Adaptive Security Appliance Software *Cisco ASA Software delivers enterprise-class security capabilities for the ASA security family in a variety of form factors.*					
Bypass	14-Jan-16	3.5	The DCERPC Inspection implementation in Cisco Adaptive Security Appliance (ASA) Software 9.4.1 through 9.5.1 allows remote authenticated users to bypass an intended DCERPC-only ACL by sending arbitrary network traffic, aka Bug ID CSCuu67782. ***Reference: CVE-2015-6423***	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160111-asa	A-CIS-ASA-220116/38
Identity Services Engine Software *ISE is a policy management and control platform for wired, wireless, and VPN.*					
Not Available	14-Jan-16	9.3	The Admin portal in Cisco Identity Services Engine (ISE) 1.1.x, 1.2.0 before patch 17, 1.2.1 before patch 8, 1.3 before patch 5, and 1.4 before patch 4 allows remote attackers to obtain administrative access via unspecified vectors, aka Bug ID CSCuw34253. ***Reference: CVE-2015-6323***	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160113-ise	A-CIS-ISE-220116/39
Wireless Lan Controller Software *Cisco Unified Wireless Network to better differentiate software releases and allow customers to choose the*					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
appropriate software release.					
Not Available	14-Jan-16	10	Cisco Wireless LAN Controller (WLC) devices with software 7.6.x, 8.0 before 8.0.121.0, and 8.1 before 8.1.131.0 allow remote attackers to change configuration settings via unspecified vectors, aka Bug ID CSCuw06153. ***Reference: CVE-2015-6314***	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160113-wlc	A-CIS-WIREL-220116/40
Colorscore Project					
Colorscore *Colorscore is a simple library that uses ImageMagick to quantize an image and find its representative colors.*					
Execute Code	08-Jan-16	10	The initialize method in the Histogram class in lib/colorscore/histogram.rb in the colorscore gem before 0.0.5 for Ruby allows context-dependent attackers to execute arbitrary code via shell metacharacters in the (1) image_path, (2) colors, or (3) depth variable. ***Reference: CVE-2015-7541***	https://github.com/quadule/colorscore/commit/570b5e854cecddd44d2047c44126aed951b61718	A-COL-COLOR-220116/41
Dell					
Pre-boot Authentication Driver *Pre-Boot Authentication (PBA) or Power-On Authentication (POA) serves as an extension of the BIOS or boot firmware and guarantees a secure, tamper-proof environment external to the operating system as a trusted authentication layer.*					
Gain Privileges	08-Jan-16	7.2	Dell Pre-Boot Authentication Driver (PBADRV.sys) 1.0.1.5 allows local users to write to arbitrary physical memory locations and gain privileges via a 0x0022201c IOCTL call. ***Reference: CVE-2015-6856***	https://www.korelogic.com/Resources/Advisories/KL-001-2015-008.txt	A-DEL-PBA-220116/42
F5					
Big-ip Access Policy Manager *APM is a flexible, high-performance access and security solution that provides unified global access to your business-critical.*					
Denial of Service; Execute Code; Overflow	12-Jan-16	9.3	F5 BIG-IP APM 11.4.1 before 11.4.1 HF9, 11.5.x before 11.5.3, and 11.6.0 before 11.6.0 HF4 allow remote attackers to cause a denial of service or execute arbitrary code via unspecified vectors related to processing a Citrix Remote Desktop connection through a virtual server configured with a remote desktop profile, aka an "Out-of-bounds memory vulnerability." ***Reference: CVE-2015-8098***	https://support.f5.com/kb/en-us/solutions/public/k/43/sol43552605.html	A-F5-BIGIP-220116/43
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 Domain Name System;Big-ip Edge Gateway;Big-ip Global Traffic Manager;Big-ip Global Traffic Manager11.2.0;Big-ip Local Traffic Manager;Big-ip Policy Enforcement Manager;Big-ip Protocol Security Module;Big-ip Wan Optimization Manager;Big-ip Webaccelerator;Big-iq Application Delivery Controller;Big-iq Centralized					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Management;Big-iq Cloud;Big-iq Cloud And Orchestration;Big-iq Device;Big-iq Security *APM is a flexible, high-performance access and security solution that provides unified global access to your business-critical.* *AFM is a high-performance, full-proxy network firewall designed to guard a data centre against incoming threats.* *Analytics (also called Application Visibility and Reporting) is a module on the BIG-IP system that lets you analyze performance of web applications.* *BIG-IP Application Acceleration Manager overcomes WAN latency, maximizes server capacity, and speeds app response times.* *Application Security Manager(ASM) is a flexible web application firewall that secures web applications in traditional, virtual, and private cloud.* *Domain Name System (DNS) is a fundamental building block for the Internet. Much like a phone book, it provides a translation service from huma readable names to computer network addresses for global systems, applications, and services across the Internet and within organizations.*					
Gain Privileges	12-Jan-16	6.9	dcoep in BIG-IP LTM, Analytics, APM, ASM, and Link Controller 11.2.0 through 11.6.0 and 12.0.0 before 12.0.0 HF1, BIG-IP AAM 11.4.0 through 11.6.0 and 12.0.0 before 12.0.0 HF1, BIG-IP AFM and PEM 11.3.0 through 11.6.0 and 12.0.0 before 12.0.0 HF1, BIG-IP DNS 12.0.0 before 12.0.0 HF1, BIG-IP Edge Gateway, WebAccelerator, and WOM 11.2.0 through 11.3.0, BIG-IP GTM 11.2.0 through 11.6.0, BIG-IP PSM 11.2.0 through 11.4.1, Enterprise Manager 3.0.0 through 3.1.1, BIG-IQ Cloud 4.0.0 through 4.5.0, BIG-IQ Device 4.2.0 through 4.5.0, BIG-IQ Security 4.0.0 through 4.5.0, BIG-IQ ADC 4.5.0, BIG-IQ Centralized Management 4.6.0, and BIG-IQ Cloud and Orchestration 1.0.0 allows local users with advanced shell (bash) access to gain privileges via unspecified vectors. ***Reference: CVE-2015-7393***	https://support.f5.com/kb/en-us/solutions/public/k/75/sol75136237.html	A-F5-BIG-I-220116/44
Not Available	12-Jan-16	9.3	BIG-IP LTM, AAM, AFM, Analytics, APM, ASM, DNS, Link Controller, and PEM 12.0.0 before HF1 on the 2000, 4000, 5000, 7000, and 10000 platforms do not properly sync passwords with the Always-On Management (AOM) subsystem, which might allow remote attackers to obtain login access to AOM via an (1) expired or (2) default password. ***Reference: CVE-2015-8611***	https://support.f5.com/kb/en-us/solutions/public/k/05/sol05272632.html	A-F5-BIG-I-220116/45
Denial of Service	12-Jan-16	4.3	BIG-IP LTM, AAM, AFM, Analytics, APM, ASM, Link Controller, and PEM 12.0.0 before HF1, when the TCP profile for a virtual server is configured with	https://support.f5.com/kb/en-us/solutions/	A-F5-BIG-I-220116/46

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Congestion Metrics Cache enabled, allow remote attackers to cause a denial of service (Traffic Management Microkernel (TMM) restart) via crafted ICMP packets, related to Path MTU (PMTU) discovery. ***Reference: CVE-2015-7759***	public/k/22/sol22843911.html	
Ffmpeg					
Ffmpeg *Ffmpeg is a very fast video and audio converter that can also grab from a live audio/video source.*					
Gain Information	14-Jan-16	4.3	FFmpeg 2.x allows remote attackers to conduct cross-origin attacks and read arbitrary files by using the concat protocol in an HTTP Live Streaming (HLS) M3U8 file, leading to an external HTTP request in which the URL string contains the first line of a local file. ***Reference: CVE-2016-1897***	http://habrahabr.ru/company/mailru/blog/274855	A-FFM-FFMPE-220116/47
Firebirdsql					
Firebird *Firebird is an open source SQL relational database management system that runs on Linux, Microsoft Windows, Mac OS X and a variety of Unix.*					
Denial of Service	13-Jan-16	4	FireBird 2.5.5 allows remote authenticated users to cause a denial of service (daemon crash) by using service manager to invoke the gbak utility with an invalid parameter. ***Reference: CVE-2016-1569***	http://sourceforge.net/p/firebird/code/62783/	A-FIR-FIREB-220116/48
Fortinet					
Forticlient *Endpoint Security Management software FortiClient is an all-in-one comprehensive security solution that extends the power of FortiGate's Unified Threat Management to endpoints on your network.*					
Gain Privileges	08-Jan-16	7.2	Fortinet FortiClient Linux SSLVPN before build 2313, when installed on Linux in a home directory that is world readable and executable, allows local users to gain privileges via the helper/subroc setuid program. ***Reference: CVE-2015-7362***	http://www.fortiguard.com/advisory/forticlient-sslvpn-linux-client-local-privilege-escalation-vulnerability	A-FOR-FORTI-220116/49
Gajim					
Gajim *Gajim is a Jabber client written in PyGTK. The goal of Gajim's developers is to provide a full featured and easy to use xmpp client for the GTK+ users.*					
Not Available	15-Jan-16	5	Gajim before 0.16.5 allows remote attackers to modify the roster and intercept messages via a crafted roster-push IQ stanza. ***Reference: CVE-2015-8688***	https://hg.gajim.org/gajim/file/gajim-0.16.5/ChangeLog	A-GAJ-GAJIM-220116/50

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
Grassroots Dicom Project					
Grassroots Dicom *Grassroots DICOM or GDCM (originally called GNU DiCoM; the name was changed at a request for integration in ITK, followed by a change in license), is a cross-platform library written in C++ for DICOM medical files*					
Denial of Service; Gain Information	12-Jan-16	6.4	The JPEGLSCodec::DecodeExtent function in MediaStorageAndFileFormat/gdcmJPEGLSCodec.cxx in Grassroots DICOM (aka GDCM) before 2.6.2 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (application crash) via an embedded JPEG-LS image with dimensions larger than the selected region in a (1) two-dimensional or (2) three-dimensional DICOM image file, which triggers an out-of-bounds read. ***Reference: CVE-2015-8397***	http://sourceforge.net/p/gdcm/gdcm/ci/e547b1ded3fd21e0b0ad149f13045aa12d4b9b7c/	A-GRA-GRASS-220116/51
Execute Code; Overflow	12-Jan-16	10	Integer overflow in the ImageRegionReader::ReadIntoBuffer function in MediaStorageAndFileFormat/gdcmImageRegionReader.cxx in Grassroots DICOM (aka GDCM) before 2.6.2 allows attackers to execute arbitrary code via crafted header dimensions in a DICOM image file, which triggers a buffer overflow. ***Reference: CVE-2015-8396***		A-GRA-GRASS-220116/52
Huawei					
Document Security Management *Document management systems commonly provide storage, versioning, metadata, security, as well as indexing and retrieval capabilities.*					
Gain Information	08-Jan-16	2.1	Huawei Document Security Management (DSM) with software before V100R002C05SPC661 does not clear the clipboard when closing a secure file, which allows local users to obtain sensitive information by pasting the contents to another file. ***Reference: CVE-2015-8303***	http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-462410.htm	A-HUA-DOCUM-220116/53
IBM					
Integration Bus;Websphere Message Broker *IBM Integration Bus (formerly known as WebSphere Message Broker) is IBM's integration broker from the WebSphere product family that allows business information to flow between disparate applications across multiple hardware and software platforms.; IBM Integration Bus (formerly known as WebSphere Message Broker) is IBM's integration broker from the WebSphere product family that allows business information to flow between disparate applications across multiple hardware and software platforms.*					
Gain Information	11-Jan-16	5	IBM WebSphere Message Broker 7 before 7.0.0.8 and 8 before 8.0.0.6 and IBM Integration Bus 9 before 9.0.0.3 and	http://www-01.ibm.com/support/docvie	A-IBM-INTEG-220116/54

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			10 before 10.0.0.0 allow remote attackers to obtain sensitive information about the HTTP server via unspecified vectors. ***Reference: CVE-2015-7399***	w.wss?uid=swg21969672	
Jazz Reporting Service *Jazz Reporting Service is an optional component of IBM Rational Reporting for Development Intelligence.*					
Bypass	09-Jan-16	4	Lifecycle Query Engine (LQE) in IBM Jazz Reporting Service (JRS) 6.0 before 6.0.0-Rational-CLM-ifix005 allows remote authenticated users to conduct LDAP injection attacks, and consequently bypass intended query restrictions or modify the LDAP directory, via unspecified vectors. ***Reference: CVE-2015-7466***	http://www-01.ibm.com/support/docview.wss?uid=swg21972484	A-IBM-JAZZ - 220116/55
Cross Site Scripting; Cross-site Request Forgery	09-Jan-16	6.8	Cross-site request forgery (CSRF) vulnerability in Lifecycle Query Engine (LQE) in IBM Jazz Reporting Service (JRS) 6.0 before 6.0.0-Rational-CLM-ifix005 allows remote authenticated users to hijack the authentication of arbitrary users for requests that insert XSS sequences. ***Reference: CVE-2015-7465***		A-IBM-JAZZ - 220116/56
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.*					
Not Available	09-Jan-16	5.8	Multiple open redirect vulnerabilities in the Aurora starter store in IBM WebSphere Commerce 7.0 through Feature Pack 8 allow remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the referrer parameter. ***Reference: CVE-2015-7397***	http://www-01.ibm.com/support/docview.wss?uid=swg24041142	A-IBM-WEBSP-220116/57
Cross Site Scripting; Cross-site Request Forgery	14-Jan-16	6.8	Cross-site request forgery (CSRF) vulnerability in IBM WebSphere Commerce 6.0 through 6.0.0.11, 7.0 through 7.0.0.9, and 7.0 Feature Pack 8 allows remote authenticated users to hijack the authentication of arbitrary users for requests that insert XSS sequences. ***Reference: CVE-2015-5007***	http://www-01.ibm.com/support/docview.wss?uid=swg21972611	A-IBM-WEBSP-220116/58
Joomla					
Joomla *Joomla! is the mobile-ready and user-friendly way to build your website.*					
Execute Code; Sql Injection	12-Jan-16	7.5	SQL injection vulnerability in Joomla! 3.x before 3.4.7 allows attackers to execute	https://developer.joomla.org	A-JOO-JOOML-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			arbitrary SQL commands via unspecified vectors. ***Reference: CVE-2015-8769***	/security-centre/640-20151207-core-sql-injection.html	220116/59
Libtiff Project					
Libtiff *Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files.*					
Denial of Service	08-Jan-16	7.5	The _TIFFVGetField function in tif_dir.c in libtiff 4.0.6 allows attackers to cause a denial of service (invalid memory write and crash) or possibly have unspecified other impact via crafted field data in an extension tag in a TIFF image. ***Reference: CVE-2015-7554***	http://www.openwall.com/lists/oss-security/2015/12/26/7	A-LIB-LIBTI-220116/60
Denial of Service; Execute Code; Overflow	08-Jan-16	7.5	Heap-based buffer overflow in the PackBitsPreEncode function in tif_packbits.c in bmp2tiff in libtiff 4.0.6 and earlier allows remote attackers to execute arbitrary code or cause a denial of service via a large width field in a BMP image. ***Reference: CVE-2015-8668***	http://packetstormsecurity.com/files/135080/libtiff-4.0.6-Heap-Overflow.html	A-LIB-LIBTI-220116/61
Mcafee					
Epolicy Orchestrator *McAfee ePolicy Orchestrator (McAfee ePO) is the most advanced, extensible, and scalable centralized security management software in the industry. Unifying security management through an open platform, McAfee ePO makes risk and compliance management simpler and more successful for organizations of all sizes*					
Execute Code	08-Jan-16	7.5	Intel McAfee ePolicy Orchestrator (ePO) 4.6.9 and earlier, 5.0.x, 5.1.x before 5.1.3 Hotfix 1106041, and 5.3.x before 5.3.1 Hotfix 1106041 allow remote attackers to execute arbitrary code via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library. ***Reference: CVE-2015-8765***	https://kc.mcafee.com/corporate/index?page=content&id=SB10144	A-MCA-EPOLI-220116/62
Microsoft					
Edge *Microsoft Edge is a web browser developed by Microsoft and included in the company's Windows 10 operating systems, replacing Internet Explorer as the default web browser on all device classes.*					
Execute Code; Overflow; Memory Corruption	13-Jan-16	9.3	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code via unspecified vectors, aka "Scripting Engine Memory Corruption Vulnerability." ***Reference: CVE-2016-0024***	http://technet.microsoft.com/en-us/security/bulletin/ms16-002	A-MIC-EDGE-220116/63
Execute Code; Overflow; Memory	13-Jan-16	9.3	Microsoft Edge allows remote attackers to execute arbitrary code via unspecified vectors, aka "Microsoft Edge Memory		A-MIC-EDGE-220116/64

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Corruption			Corruption Vulnerability." ***Reference: CVE-2016-0003***		
Exchange Server *Microsoft Exchange Server is a calendaring and mail server developed by Microsoft that runs exclusively on the Microsoft Windows Server product line.*					
Cross Site Scripting	13-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in Outlook Web Access (OWA) in Microsoft Exchange Server 2013 PS1, 2013 Cumulative Update 10, 2013 Cumulative Update 11, and 2016 allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka "Exchange Spoofing Vulnerability." ***Reference: CVE-2016-0032***	http://technet.microsoft.com/en-us/security/bulletin/ms16-010	A-MIC-EXCHA-220116/65
Cross Site Scripting	13-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in Outlook Web Access (OWA) in Microsoft Exchange Server 2016 allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka "Exchange Spoofing Vulnerability," a different vulnerability than CVE-2016-0029. ***Reference: CVE-2016-0031***		A-MIC-EXCHA-220116/66
Cross Site Scripting	13-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in Outlook Web Access (OWA) in Microsoft Exchange Server 2013 PS1, 2013 Cumulative Update 10, and 2016 allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka "Exchange Spoofing Vulnerability." ***Reference: CVE-2016-0030***		A-MIC-EXCHA-220116/67
Cross Site Scripting	13-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in Outlook Web Access (OWA) in Microsoft Exchange Server 2016 allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka "Exchange Spoofing Vulnerability," a different vulnerability than CVE-2016-0031. ***Reference: CVE-2016-0029***		A-MIC-EXCHA-220116/68
Internet Explorer *Internet Explorer[a] (formerly Microsoft Internet Explorer[b] and Windows Internet Explorer,[c] commonly abbreviated IE or MSIE) is a series of graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating systems*					
Bypass	13-Jan-16	4.3	Microsoft Internet Explorer 9 through 11 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability." ***Reference: CVE-2016-0005***	http://technet.microsoft.com/en-us/security/bulletin/ms16-001	A-MIC-INTER-220116/69
Jscript;Vbscript *JScript and Visual Basic Scripting Edition (VBScript) are scripting languages that can be used in Windows-based applications.*					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Execute Code; Overflow; Memory Corruption	13-Jan-16	9.3	The Microsoft (1) VBScript 5.7 and 5.8 and (2) JScript 5.7 and 5.8 engines, as used in Internet Explorer 8 through 11 and other products, allow remote attackers to execute arbitrary code via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." ***Reference: CVE-2016-0002***	http://technet.microsoft.com/en-us/security/bulletin/ms16-001	A-MIC-JSCRI-220116/70
Sharepoint Foundation;Sharepoint Server *SharePoint Foundation (formerly Windows SharePoint Services) is free for on-premises deployment. You can use SharePoint Foundation to create many types of sites where you can collaborate on webpages, documents, lists, calendars, and data.* *SharePoint is a web application platform in the Microsoft Office server suite. SharePoint combines various functions which are traditionally separate applications: intranet, extranet, content management, document management etc.*					
Cross Site Scripting; Bypass	13-Jan-16	3.5	Microsoft SharePoint Server 2013 SP1 and SharePoint Foundation 2013 SP1 allow remote authenticated users to bypass intended Access Control Policy restrictions and conduct cross-site scripting (XSS) attacks by modifying a webpart, aka "Microsoft SharePoint Security Feature Bypass," a different vulnerability than CVE-2015-6117. ***Reference: CVE-2016-0011***	http://technet.microsoft.com/en-us/security/bulletin/ms16-004	A-MIC-SHARE-220116/71
Cross Site Scripting; Bypass	13-Jan-16	4.3	Microsoft SharePoint Server 2013 SP1 and SharePoint Foundation 2013 SP1 allow remote authenticated users to bypass intended Access Control Policy restrictions and conduct cross-site scripting (XSS) attacks by modifying a webpart, aka "Microsoft SharePoint Security Feature Bypass," a different vulnerability than CVE-2016-0011. ***Reference: CVE-2015-6117***		A-MIC-SHARE-220116/72
Silverlight *Silverlight is a powerful development tool for creating engaging, interactive user experiences for Web and mobile applications*					
Denial of Service; Execute Code	13-Jan-16	9.3	Microsoft Silverlight 5 before 5.1.41212.0 mishandles negative offsets during decoding, which allows remote attackers to execute arbitrary code or cause a denial of service (object-header corruption) via a crafted web site, aka "Silverlight Runtime Remote Code Execution Vulnerability." ***Reference: CVE-2016-0034***	http://technet.microsoft.com/en-us/security/bulletin/ms16-006	A-MIC-SILVE-220116/73
Nghttp2					
Nghttp2 *HTTP/2 C Library and tools*					
Not Available	12-Jan-16	9.3	The idle stream handling in nghttp2	https://nghttp	A-NGH-

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 1.6.0 allows attackers to have unspecified impact via unknown vectors, aka a heap-use-after-free bug. ***Reference: CVE-2015-8659***	2.org/blog/2015/12/23/nghttp2-v1-6-0/	NGHTT-220116/74
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.*					
Gain Information	14-Jan-16	4	The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key. ***Reference: CVE-2016-0777***	http://www.openssh.com/txt/release-7.1p2	A-OPE-OPENS-220116/75
Opencart					
Opencart *OpenCart is an open source PHP-based online e-commerce solution.*					
Cross Site Scripting	12-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in OpenCart before 2.1.0.2 allows remote attackers to inject arbitrary web script or HTML via the zone_id parameter to index.php. ***Reference: CVE-2015-4671***	https://github.com/opencart/opencart/commit/303fa88fe664ded4bf8753b997abd916f0a3c03f	A-OPE-OPENC-220116/76
Openstack					
Compute *OpenStack Compute service is used for hosting and managing cloud computing systems*					
Not Available	12-Jan-16	2.1	OpenStack Compute (Nova) before 2015.1.3 (kilo) and 12.0.x before 12.0.1 (liberty), when using libvirt to spawn instances and use_cow_images is set to false, allow remote authenticated users to read arbitrary files by overwriting an instance disk with a crafted image and requesting a snapshot. ***Reference: CVE-2015-7548***	https://security.openstack.org/ossa/OSSA-2016-001.html	A-OPE-COMPU-220116/77
Owncloud					
Owncloud *OwnCloud is open source software Which provides a file synchronization and sharing solution on servers that you control.*					
Gain Information	08-Jan-16	3.5	ownCloud Server before 7.0.12, 8.0.x before 8.0.10, 8.1.x before 8.1.5, and 8.2.x before 8.2.2, when the "file_versions" application is enabled, does not properly check the return value of getOwner, which allows remote authenticated users to read the files with names starting with	https://owncloud.org/security/advisory/?id=oc-sa-2016-003	A-OWN-OWNCL-220116/78

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			".v" and belonging to a sharing user by leveraging an incoming share. ***Reference: CVE-2016-1500***		
Gain Information	08-Jan-16	4	ownCloud Server before 8.0.9 and 8.1.x before 8.1.4 allow remote authenticated users to obtain sensitive information via unspecified vectors, which reveals the installation path in the resulting exception messages. ***Reference: CVE-2016-1501***	https://owncloud.org/security/advisory/?id=oc-sa-2016-004	A-OWN-OWNCL-220116/79
Cross Site Scripting	08-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in the OCS discovery provider component in ownCloud Server before 7.0.12, 8.0.x before 8.0.10, 8.1.x before 8.1.5, and 8.2.x before 8.2.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors involving a URL. ***Reference*: CVE-2016-1498**	https://owncloud.org/security/advisory/?id=oc-sa-2016-001	A-OWN-OWNCL-220116/80
Denial of Service; Gain Information	08-Jan-16	7.5	ownCloud Server before 8.0.10, 8.1.x before 8.1.5, and 8.2.x before 8.2.2 allow remote authenticated users to obtain sensitive information from a directory listing and possibly cause a denial of service (CPU consumption) via the force parameter to index.php/apps/files/ajax/scan.php. ***Reference: CVE-2016-1499***	https://owncloud.org/security/advisory/?id=oc-sa-2016-002	A-OWN-OWNCL-220116/81
Pearl					
Pathtools *Path Tools is a package containing two powerful plug-ins, Rakka and Wiggle Stroke. These plug-ins are targeted at creating animations based on mask paths*					
Bypass	13-Jan-16	7.5	The canonpath function in the File::Spec module in PathTools before 3.62, as used in Perl, does not properly preserve the taint attribute of data, which might allow context-dependent attackers to bypass the taint protection mechanism via a crafted string. ***Reference: CVE-2015-8607***	https://rt.perl.org/Public/Bug/Display.html?id=126862	A-PEA-PATHT-220116/82
Phusionpassenger					
Phusion Passenger *Phusion Passenger is a multi-language (Ruby, Python, Node) web & app server which can integrate into Apache and Nginx.*					
Not Available	08-Jan-16	4.3	agent/Core/Controller/SendRequest.cpp in Phusion Passenger before 4.0.60 and 5.0.x before 5.0.22, when used in Apache integration mode or in standalone mode without a filtering proxy, allows remote attackers to spoof headers passed to applications by using an _ (underscore) character instead of a - (dash) character	https://blog.phusion.nl/2015/12/07/cve-2015-7519/	A-PHU-PHUSI-220116/83

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			in an HTTP header, as demonstrated by an X_User header. ***Reference: CVE-2015-7519***		
Puppetlabs					
Puppet Enterprise *Puppet Enterprise helps you make rapid, repeatable changes and automatically enforce the consistency of systems and devices–across physical and virtual.*					
Gain Information	08-Jan-16	1.9	Puppet Server in Puppet Enterprise before 3.8.x before 3.8.3 and 2015.2.x before 2015.2.3 uses world-readable permissions for the private key of the Certification Authority (CA) certificate during the initial installation and configuration, which might allow local users to obtain sensitive information via unspecified vectors. ***Reference: CVE-2015-7328***	https://puppetlabs.com/security/cve/cve-2015-7328	A-PUP-PUPPE-220116/84
Python					
Python *Python is a widely used general-purpose, high-level programming language. Its design philosophy emphasizes code readability, and its syntax allows programmers to express concepts in fewer lines of code than would be possible in languages such as C++ or Java*					
Not Available	13-Jan-16	5	The verify function in the RSA package for Python (Python-RSA) before 3.3 allows attackers to spoof signatures with a small public exponent via crafted signature padding, aka a BERserk attack. ***Reference: CVE-2016-1494***	https://bitbucket.org/sybren/python-rsa/pull-requests/14/security-fix-bb06-attack-in-verify-by/diff	A-PYT-PYTHO-220116/85
Qemu					
Qemu *QEMU (short for Quick Emulator) is a free and open-source hosted hypervisor that performs hardware virtualization*					
Denial of Service; Execute Code; Overflow	08-Jan-16	6.8	Buffer overflow in the pcnet_receive function in hw/net/pcnet.c in QEMU, when a guest NIC has a larger MTU, allows remote attackers to cause a denial of service (guest OS crash) or execute arbitrary code via a large packet. ***Reference: CVE-2015-7512***	http://git.qemu.org/?p=qemu.git;a=commit;h=8b98a2f07175d46c3f7217639bd5e03f	A-QEM-QEMU-220116/86
Redhen Project					
Redhen *RedHen is a Drupal-native CRM initially designed for common nonprofit needs, but built for flexibility*					
Cross Site Scripting	15-Jan-16	3.5	Multiple cross-site scripting (XSS) vulnerabilities in the Redhen module 7.x-1.x before 7.x-1.11 for Drupal allow remote authenticated users with certain access to inject arbitrary web script or	https://www.drupal.org/node/2649780	A-RED-REDHE-220116/87

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
			HTML via unspecified vectors, related to (1) individual contacts, (2) notes, or (3) engagement scores. ***Reference: CVE-2016-1913***		
S9Y					
Serendipity *Serendipity is a PHP-powered weblog application which gives the user an easy way to maintain an online diary, weblog or even a complete homepage*					
Cross Site Scripting	12-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in Serendipity before 2.0.3 allows remote attackers to inject arbitrary web script or HTML via the serendipity[entry_id] parameter in an "edit" admin action to serendipity_admin.php. ***Reference: CVE-2015-8603***	http://blog.s9y.org/archives/266-Serendipity-2.0.3-released.html	A-S9Y-SEREN-220116/88
Samsung					
Web Viewer *WebViewer is a Windows application, which permits the playback of certain live video streams and video archives with synchronized sides and TabletPC ink.*					
Bypass	14-Jan-16	7.8	Web Viewer 1.0.0.193 on Samsung SRN-1670D devices allows attackers to bypass filesystem encryption via XOR calculations. ***Reference: CVE-2015-8281***	https://www.kb.cert.org/vuls/id/913000	A-SAM-WEBV-220116/89
Not Available	14-Jan-16	5	Web Viewer 1.0.0.193 on Samsung SRN-1670D devices allows remote attackers to read arbitrary files via a request to an unspecified PHP script. ***Reference: CVE-2015-8279***		A-SAM-WEBV-220116/90
Netweaver *NetWeaver is an application builder from SAP for integrating business processes and databases from a number of sources while exploiting the leading Web services technologies.*					
Cross Site Scripting	15-Jan-16	4.3	Multiple cross-site scripting (XSS) vulnerabilities in SAP NetWeaver 7.4 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors to the (1) Runtime Workmench (RWB) or (2) Pmitest servlet in the Process Monitoring Infrastructure (PMI), aka SAP Security Note 2206793 and 2234918. ***Reference: CVE-2016-1911***	http://erpscan.com/advisories/erpscan-16-001-xss-sap-netweaver-7-4-mdt-servlet/	A-SAP-NETWE-220116/91
Symphony-cms					
Symphony Cms *Symphony is an XSLT-powered open source content management system.*					
Cross Site Scripting	08-Jan-16	4.3	Multiple cross-site scripting (XSS) vulnerabilities in content/content.systempreferences.php in Symphony CMS before 2.6.4 allow remote attackers to inject arbitrary web	http://www.getsymphony.com/download/releases/version/2.6.4/	A-SYM-SYMPH-220116/92

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			script or HTML via the (1) email_sendmail[from_name], (2) email_sendmail[from_address], (3) email_smtp[from_name], (4) email_smtp[from_address], (5) email_smtp[host], (6) email_smtp[port], (7) jit_image_manipulation[trusted_external_sites], or (8) maintenance_mode[ip_whitelist] parameters to system/preferences. ***Reference: CVE-2015-8766***		
Cross Site Scripting	08-Jan-16	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Symphony CMS 2.6.3 allow remote attackers to inject arbitrary web script or HTML via the (1) Name, (2) Navigation Group, or (3) Label parameter to blueprints/sections/edit/1. ***Reference: CVE-2015-8376***	http://seclists.org/fulldisclosure/2015/Dec/7	A-SYM-SYMPH-220116/93
Typo3					
Typo3 *TYPO3 is a free and open source web content management system based on PHP.*					
Cross Site Scripting	08-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in the typoLink function in TYPO3 6.2.x before 6.2.16 and 7.x before 7.6.1 allows remote authenticated editors to inject arbitrary web script or HTML via a link field. ***Reference: CVE-2015-8759***	http://typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2015-012/	A-TYP-TYPO3-220116/94
Cross Site Scripting	08-Jan-16	3.5	Multiple cross-site scripting (XSS) vulnerabilities in unspecified frontend components in TYPO3 6.2.x before 6.2.16 and 7.x before 7.6.1 allow remote authenticated editors to inject arbitrary web script or HTML via unknown vectors. ***Reference: CVE-2015-8758***	http://typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2015-013/	A-TYP-TYPO3-220116/95
Cross Site Scripting	08-Jan-16	3.5	Cross-site scripting (XSS) vulnerability in the search result view in the Indexed Search (indexed_search) component in TYPO3 6.2.x before 6.2.16 allows remote authenticated editors to inject arbitrary web script or HTML via unspecified vectors. ***Reference: CVE-2015-8756***	http://typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2015-015/	A-TYP-TYPO3-220116/96
Cross Site Scripting	08-Jan-16	3.5	Multiple cross-site scripting (XSS) vulnerabilities in unspecified backend components in TYPO3 6.2.x before 6.2.16 and 7.x before 7.6.1 allow remote authenticated editors to inject arbitrary	http://typo3.org/teams/security/security-bulletins/typo3-core/typo3-	A-TYP-TYPO3-220116/97

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			web script or HTML via unknown vectors. ***Reference: CVE-2015-8755***	core-sa-2015-011/	
Cross Site Scripting	08-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in the Extension Manager in TYPO3 6.2.x before 6.2.16 and 7.x before 7.6.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to extension data during an extension installation. ***Reference: CVE-2015-8757***	http://typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2015-010/	A-TYP-TYPO3-220116/98
Not Available	08-Jan-16	4.3	The Flvplayer component in TYPO3 6.2.x before 6.2.16 allows remote attackers to embed Flash videos from external domains via unspecified vectors, aka "Cross-Site Flashing." ***Reference: CVE-2015-8760***	http://typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2015-014/	A-TYP-TYPO3-220116/99
Unitronics					
Visilogic Oplc Ide *PLC + HMI · The All-In-One Control Solution*					
Execute Code; Overflow	08-Jan-16	9.3	Heap-based buffer overflow in Unitronics VisiLogic OPLC IDE before 9.8.09 allows remote attackers to execute arbitrary code via a long vlp filename. ***Reference: CVE-2015-7939***	http://www.zerodayinitiative.com/advisories/ZDI-16-001	A-UNI-VISIL-220116/100
Operating System (OS)					
Advantech					
Eki-1321 Series Firmware *EKI-1321 cellular gateways can transparently bring RS-232/422/485 or Ethernet devices to a cellular network. They allow nearly any device with serial or Ethernet ports to connect and share a cellular network with easy and simple configuration.*					
Bypass	08-Jan-16	9.3	Advantech EKI-132x devices with firmware before 2015-12-31 allow remote attackers to bypass authentication via unspecified vectors. ***Reference: CVE-2015-7938***	https://ics-cert.us-cert.gov/advisories/ICSA-15-344-01	OS-ADV-EKI-220116/101
Apple					
Apple Tv;Iphone Os;Mac Os X *Apple TV is an HDMI-compliant source device.* *Ios (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.* *Mac OS X, is a series of Unix-based graphical interface operating systems developed and marketed by Apple Inc. It is designed to run on Mac computers, having been pre-installed on all Macs since 2002.*					
Denial of Service; Overflow; Memory Corruption;	09-Jan-16	4.3	libxml2 in Apple iOS before 9.2, OS X before 10.11.2, and tvOS before 9.1 allows remote attackers to obtain sensitive information or cause a denial of service (memory corruption) via a	https://support.apple.com/HT205640	OS-APP-APPLE-220116/102

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Gain Information			crafted XML document, a different vulnerability than CVE-2015-7115. ***Reference: CVE-2015-7116***		
Denial of Service; Overflow; Memory Corruption; Gain Information	09-Jan-16	4.3	libxml2 in Apple iOS before 9.2, OS X before 10.11.2, and tvOS before 9.1 allows remote attackers to obtain sensitive information or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2015-7116. ***Reference: CVE-2015-7115***		OS-APP-APPLE-220116/103
Mac Os X *Mac OS X, is a series of Unix-based graphical interface operating systems developed and marketed by Apple Inc. It is designed to run on Mac computers, having been pre-installed on all Macs since 2002.*					
Gain Privileges; Bypass	11-Jan-16	6.9	Untrusted search path vulnerability in Apple OS X before 10.11.1 allows local users to bypass intended Gatekeeper restrictions and gain privileges via a Trojan horse program that is loaded from an unexpected directory by an application that has a valid Apple digital signature. ***Reference: CVE-2015-7024***	https://support.apple.com/HT205375	OS-APP-MACOS-220116/104
Gain Privileges	11-Jan-16	7.2	Directory Utility in Apple OS X before 10.11.1 mishandles authentication for new sessions, which allows local users to gain privileges via unspecified vectors. ***Reference: CVE-2015-6980***		OS-APP-MACOS-220116/105
Cisco					
Aironet Access Point Software *Cisco Aironet Series wireless access points are easily deployed in networks for a branch offices, campuses, or large enterprises. They are highly secure network.*					
Denial of Service	14-Jan-16	7.8	The IP ingress packet handler on Cisco Aironet 1800 devices with software 8.1(112.3) and 8.1(112.4) allows remote attackers to cause a denial of service via a crafted header in an IP packet, aka Bug ID CSCuv63138. ***Reference: CVE-2015-6320***	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160113-aironet	OS-CIS-AIRON-220116/106
Not Available	14-Jan-16	7.5	Cisco Aironet 1800 devices with software 7.2, 7.3, 7.4, 8.1(112.3), 8.1(112.4), and 8.1(15.14) have a default account, which makes it easier for remote attackers to obtain access via unspecified vectors, aka Bug ID CSCuw58062. ***Reference: CVE-2015-6336***	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160113-air	OS-CIS-AIRON-220116/107
Huawei					
Te60 Firmware *Huawei TE60 is the top-of-the-line HD video conferencing endpoint, offering the largest array of audio/video*					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
interfaces and Wi-Fi connection with fully featured multi-view image sending.					
Denial of Service	12-Jan-16	5	The presentation transmission permission management mechanism in Huawei TE30, TE40, TE50, and TE60 multimedia video conferencing endpoints with software before V100R001C10SPC100 allows remote attackers to cause a denial of service (wired presentation outage) via unspecified vectors involving to a wireless presentation. ***Reference: CVE-2015-8672***	http://www.huawei.com/en/psirt/security-advisories/hw-462952	OS-HUA-TE60 - 220116/108
Juniper					
Screenos					
ScreenOS is a real-time embedded operating system for the NetScreen range of hardware firewall devices from Juniper Networks.					
Denial of Service; Execute Code	08-Jan-16	9.3	Juniper ScreenOS before 6.3.0r21, when ssh-pka is configured and enabled, allows remote attackers to cause a denial of service (system crash) or execute arbitrary code via crafted SSH negotiation. ***Reference: CVE-2015-7754***	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10712	OS-JUN-SCREE-220116/109
Microsoft					
Windows 10					
Bypass	13-Jan-16	9.3	The Remote Desktop Protocol (RDP) service implementation in Microsoft Windows 10 Gold and 1511 allows remote attackers to bypass intended access restrictions and establish sessions for blank-password accounts via a modified RDP client, aka "Windows Remote Desktop Protocol Security Bypass Vulnerability." ***Reference: CVE-2016-0019***	http://technet.microsoft.com/en-us/security/bulletin/ms16-007	OS-MIC-WINDO-220116/110
Windows 10;Windows 7;Windows 8;Windows 8.1;Windows Rt;Windows Rt 8.1;Windows Server 2008;Windows Server 2012					
Execute Code; Gain Privileges	13-Jan-16	6.9	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka "DLL Loading Remote Code Execution Vulnerability." ***Reference: CVE-2016-0016***	http://technet.microsoft.com/en-us/security/bulletin/ms16-007	OS-MIC-WINDO-220116/111
Gain Privileges	13-Jan-16	6.9	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT		OS-MIC-WINDO-220116/112

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
			Gold and 8.1, and Windows 10 Gold and 1511 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka "DLL Loading Elevation of Privilege Vulnerability." ***Reference: CVE-2016-0014***		
Gain Privileges	13-Jan-16	6.9	The sandbox implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandles reparse points, which allows local users to gain privileges via a crafted application, aka "Windows Mount Point Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0006. ***Reference: CVE-2016-0007***	http://technet.microsoft.com/en-us/security/bulletin/ms16-008	OS-MIC-WINDO-220116/113
Gain Privileges	13-Jan-16	6.9	The sandbox implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandles reparse points, which allows local users to gain privileges via a crafted application, aka "Windows Mount Point Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0007. ***Reference: CVE-2016-0006***		OS-MIC-WINDO-220116/114
Execute Code; Overflow	13-Jan-16	9.3	DirectShow in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted file, aka "DirectShow Heap Corruption Remote Code Execution Vulnerability." ***Reference: CVE-2016-0015***	http://technet.microsoft.com/en-us/security/bulletin/ms16-007	OS-MIC-WINDO-220116/115
Execute Code; Gain Privileges	13-Jan-16	6.9	Microsoft Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 R2, and Windows 10 Gold and 1511 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka "DLL Loading Remote Code Execution Vulnerability." ***Reference: CVE-2016-0018***		OS-MIC-WINDO-220116/116
Execute Code	13-Jan-16	9.3	Microsoft Windows Vista SP2, Windows	http://technet	OS-MIC-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Server 2008 SP2 and R2 SP1, Windows 7 SP1, and Windows 10 Gold and 1511 allow remote attackers to execute arbitrary code via unspecified vectors, aka "Win32k Remote Code Execution Vulnerability." ***Reference: CVE-2016-0009***	.microsoft.com /en-us/security/bulletin/ms16-005	WINDO-220116/117
Bypass; Gain Information	13-Jan-16	4.3	The graphics device interface in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to bypass the ASLR protection mechanism via unspecified vectors, aka "Windows GDI32.dll ASLR Bypass Vulnerability." ***Reference: CVE-2016-0008***		OS-MIC-WINDO-220116/118
Gain Privileges	13-Jan-16	7.2	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 mishandle DLL loading, which allows local users to gain privileges via a crafted application, aka "MAPI DLL Loading Elevation of Privilege Vulnerability." ***Reference: CVE-2016-0020***	http://technet .microsoft.com /en-us/security/bulletin/ms16-007	OS-MIC-WINDO-220116/119
Mozilla					
Firefox Os *Firefox OS(project name: Boot to Gecko, also known as B2G) is an open-source operating system – made for smartphones, tablet computers and smart Tvs – designed by Mozilla and external contributors, based on the rendering engine of their Firefox web browser and the Linux kernel.*					
Not Available	08-Jan-16	2.1	The lockscreen feature in Mozilla Firefox OS before 2.5 does not properly restrict failed authentication attempts, which makes it easier for physically proximate attackers to obtain access by entering many passcode guesses. ***Reference: CVE-2015-8512***	https://bugzilla.mozilla.org/show_bug.cgi?id=1181571	OS-MOZ-FIREF-220116/120
Cross Site Scripting	08-Jan-16	4.3	Cross-site scripting (XSS) vulnerability in the internationalization feature in the default homescreen app in Mozilla Firefox OS before 2.5 allows user-assisted remote attackers to inject arbitrary web script or HTML via a crafted web site that is mishandled during "Add to home screen" bookmarking. ***Reference: CVE-2015-8510***	https://bugzilla.mozilla.org/show_bug.cgi?id=1190038	OS-MOZ-FIREF-220116/121
Bypass	08-Jan-16	6.9	Race condition in the lockscreen feature in Mozilla Firefox OS before 2.5 allows physically proximate attackers to bypass	https://bugzilla.mozilla.org/show_bug.cgi?i	OS-MOZ-FIREF-220116/122

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
			an intended passcode requirement via unspecified vectors. ***Reference: CVE-2015-8511***	d=1173284	
XEN					
XEN *Xen Project is an open-source type-1 or baremetal hypervisor, which makes it possible to run many instances of an operating system or indeed different operating systems in parallel on a single machine (or host).*					
Denial of Service	08-Jan-16	2.1	The hvm_set_callback_via function in arch/x86/hvm/irq.c in Xen 4.6 does not limit the number of printk console messages when logging the new callback method, which allows local HVM guest OS users to cause a denial of service via a large number of changes to the callback method (HVM_PARAM_CALLBACK_IRQ). ***Reference: CVE-2015-8615***	http://xenbits.xen.org/xsa/advisory-169.html	OS-XEN-XEN-220116/123
Operating System/Application (OS/A)					
Apache/Fedoraproject					
Activemq/Fedora *Apache ActiveMQ is an open source message broker written in Java together with a full Java Message Service (JMS) client.* *Fedora is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat.*					
Execute Code	08-Jan-16	7.5	Apache ActiveMQ 5.x before 5.13.0 does not restrict the classes that can be serialized in the broker, which allows remote attackers to execute arbitrary code via a crafted serialized Java Message Service (JMS) ObjectMessage object. ***Reference:*** **CVE-2015-5254**	http://activemq.apache.org/security-advisories.data/CVE-2015-5254-announcement.txt	OS-A-APA-ACTIV-220116/124
Gummi Project/Novell					
Gummi/Leap;Opensuse *Gummi is a LaTeX editor. It is a GTK+ application which runs on Linux and Windows systems.* *Creating usable open-source tools for software developers and system administrators, while providing a user-friendly desktop, and feature-rich server environment.*					
Not Available	08-Jan-16	2.1	Gummi 0.6.5 allows local users to write to arbitrary files via a symlink attack on a temporary dot file that uses the name of an existing file and a (1) .aux, (2) .log, (3) .out, (4) .pdf, or (5) .toc extension for the file name, as demonstrated by .thesis.tex.aux. ***Reference: CVE-2015-7758***	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=756432	OS-A-GUM-GUMMI-220116/125
Fedoraproject; Shellinabox Project					
Fedora; Shell in a box *Shell In A Box implements a web server that can export arbitrary command line tools to a web based terminal emulator.*					
Not Available	12-Jan-16	4.3	The HTTPS fallback implementation in Shell In A Box (aka shellinabox) before	https://github.com/shellina	OS-A-FED-FEDOR-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			2.19 makes it easier for remote attackers to conduct DNS rebinding attacks via the "/plain" URL. ***Reference: CVE-2015-8400***	box/shellinabox/releases/tag/v2.19	220116/126
Vmware					
Esxi; Fusion; Player; Workstation *VMware ESXi (formerly ESX) is an enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers* *VMware Fusion is a software hypervisor developed by VMware for computers running OS X with Intel processors.* *VMware Workstation Player is the best way to deliver virtual machines and multiple operating systems;*					
Denial of Service; Gain Privileges; Memory Corruption	08-Jan-16	6.5	The VMware Tools HGFS (aka Shared Folders) implementation in VMware Workstation 11.x before 11.1.2, VMware Player 7.x before 7.1.2, VMware Fusion 7.x before 7.1.2, and VMware ESXi 5.0 through 6.0 allows Windows guest OS users to gain guest OS privileges or cause a denial of service (guest OS kernel memory corruption) via unspecified vectors. ***Reference: CVE-2015-6933***	http://www.vmware.com/security/advisories/VMSA-2016-0001.html	OS-A-VMW-ESXI-220116/127
Canonical/Pygments					
Ubuntu Linux/Pygments *Ubuntu is an open source software platform that runs everywhere from the smartphone, the tablet and the PC to the server and the cloud.* *Pygments is a generic syntax highlighter for general use in all kinds of software such as forum systems, wikis or other applications that need to prettify source code.*					
Execute Code	08-Jan-16	9.3	The FontManager._get_nix_font_path function in formatters/img.py in Pygments 1.2.2 through 2.0.2 allows remote attackers to execute arbitrary commands via shell metacharacters in a font name. ***Reference: CVE-2015-8557***	http://www.ubuntu.com/usn/USN-2862-1	OS-A-CAN-UBUNT-220116/128
Fedoraproject/Zarafa					
Fedora/Zarafa Collaboration Platform *The Zarafa Collaboration Platform (ZCP) is a Microsoft Exchange replacement. The Open Source Collaboration provides an integration with your existing Linux mail server and native mobile phone support by ActiveSync compatibility*					
Gain Privileges	11-Jan-16	7.2	zarafa-autorespond in Zarafa Collaboration Platform (ZCP) before 7.2.1 allows local users to gain privileges via a symlink attack on /tmp/zarafa-vacation-*. ***Reference: CVE-2015-6566***	https://download.zarafa.com/community/final/7.2/final-changelog-7.2.txt	OS-A-FED-FEDOR-220116/129
Novell/Quassel-irc					
Leap; Opensuse/Quassel *Creating usable open-source tools for software developers and system administrators, while providing a user-friendly desktop, and feature-rich server environment.;*					

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
Quassel IRC is a modern, cross-platform, distributed IRC client, meaning that one (or multiple) client(s) can attach to and detach from a central core -- much like the popular combination of screen and a text-based IRC client such as WeeChat, but graphical.					
Denial of Service	08-Jan-16	5	The CoreUserInputHandler::doMode function in core/coreuserinputhandler.cpp in Quassel 0.10.0 allows remote attackers to cause a denial of service (application crash) via the "/op *" command in a query. ***Reference: CVE-2015-8547***	https://github.com/quassel/quassel/pull/153	OS-A-NOV-LEAP-220116/130
Operating System/Hardware (OS/H)					
Huawei					
Te30; Te60 Firmware *HUAWEI TE30 is an all-in-one HD videoconferencing system with unique voice dialing.* *Huawei TE60 is the top-of-the-line HD video conferencing endpoint, offering the largest array of audio/video interfaces and Wi-Fi connection with fully featured multi-view image sending.*					
Not Available	12-Jan-16	4.6	The mod_dialback module in Prosody before 0.9.9 does not properly generate random values for the secret token for server-to-server dialback authentication, which makes it easier for attackers to spoof servers via a brute force attack. ***Reference: CVE-2016-1232***	http://blog.prosody.im/prosody-0-9-9-security-release/	OS-H-HUA-TE30-220116/131