National Critical Information Infrastructure Protection Centre

CVE Report

16- 30 June 2016 **Vol. 3 No.11**

Product/ Vulnerability Type(s)	Publish Date	CVSS	Description	Patch	NCIIPC ID
Application(A)					
Libreswan					
Libreswan *Libreswan is a free software implementation of the most widely supported and standardized VPN protocol based on IPsec and the Internet Key Exchange (IKE). These standards are produced and maintained by the Internet Engineering Task Force (IETF).*					
Denial of Service	2016-06-16	5	programs/pluto/ikev1.c in libreswan before 3.17 retransmits in initial-responder states, which allows remote attackers to cause a denial of service (traffic amplification) via a spoofed UDP packet. NOTE: the original behavior complies with the IKEv1 protocol, but has a required security update from the libreswan vendor; as of 2016-06-10, it is expected that several other IKEv1 implementations will have vendor-required security updates, with separate CVE IDs assigned to each. **Reference: CVE-2016-5361**	https://github.com/libreswan/libreswan/commit/152d6d95632d8b9477c170f1de99bcd86d7fb1d6	A-LIB-LIBRE-80716/1
Adobe					
Flash Player *Adobe Flash Player is the high performance, lightweight, highly expressive client runtime that delivers powerful and consistent user experiences across major operating systems, browsers, mobile phones and devices.*					
Execute Code	2016-06-16	10	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier allows remote attackers to execute arbitrary code via unknown vectors, as exploited in the wild in June 2016.	https://helpx.adobe.com/security/products/flash-player/apsa16-03.html	A-ADO-FLASH-80716/2

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

			Reference: CVE-2016-4171		
Dng Software Development Kit *The Adobe DNG SDK provides support for reading and writing DNG files as well as support for converting DNG data into a format easily displayed or processed by imaging applications.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-06-16	7.5	Adobe DNG Software Development Kit (SDK) before 1.4 2016 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference: CVE-2016-4167**	https://helpx.adobe.com/security/products/dng-sdk/apsb16-19.html	A-ADO-DNG S-80716/3
Flash Player *Adobe Flash Player is the high performance, lightweight, highly expressive client runtime that delivers powerful and consistent user experiences across major operating systems, browsers, mobile phones and devices.*					
NA	2016-06-16	10	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4166**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/4
Brackets *Brackets is a free open-source editor written in HTML, CSS, and JavaScript with a primary focus on Web Development.*					
NA	2016-06-16	10	The extension manager in Adobe Brackets before 1.7 allows attackers to have an unspecified impact via invalid input. **Reference: CVE-2016-4165**	https://helpx.adobe.com/security/products/brackets/apsb16-20.html	A-ADO-BRACK-80716/5
Cross Site Scripting	2016-06-16	4.3	Cross-site scripting (XSS) vulnerability in Adobe Brackets before 1.7 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-4164**	https://helpx.adobe.com/security/products/brackets/apsb16-20.html	A-ADO-BRACK-80716/6
Air Desktop Runtime;Air Sdk;Air Sdk & Compiler;Flash Player *Adobe AIR (Adobe Integrated Runtime) is a developer's tool for creating platform-independent web*					

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

applications that can be run on a user's desktop. The Adobe AIR SDK provides the tools necessary to build and deploy Adobe AIR applications. Adobe AIR SDK & Compiler provides developers with a consistent and flexible development environment for the delivery of out-of-browser applications and games across devices and platforms (Windows, Mac, iOS, Android). Adobe Flash Player is the high performance, lightweight, highly expressive client runtime that delivers powerful and consistent user experiences across major operating systems, browsers, mobile phones and devices.					
Denial of Service; Execute Code; Overflow ; Memory Corruption	2016-06-16	7.5	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4120, CVE-2016-4160, CVE-2016-4161, and CVE-2016-4162. **Reference: CVE-2016-4163**	https://helpx.adobe.com/security/products/flash-player/apsb16-15.html	A-ADO-AIR D-80716/7
Denial of Service; Execute Code; Overflow ;Memory Corruption	2016-06-16	7.5	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4120, CVE-2016-4160, CVE-2016-4161, and CVE-2016-4163.	https://helpx.adobe.com/security/products/flash-player/apsb16-15.html	A-ADO-AIR D-80716/8

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

			Reference: CVE-2016-4162		
Denial of Service ; Execute Code; Overflow; Memory Corruption	2016-06-16	7.5	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4120, CVE-2016-4160, CVE-2016-4162, and CVE-2016-4163. **Reference: CVE-2016-4161**	https://helpx.adobe.com/security/products/flash-player/apsb16-15.html	A-ADO-AIR D-80716/9
Denial of Service ; Execute Code; Overflow ;Memory Corruption	2016-06-16	7.5	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4120, CVE-2016-4161, CVE-2016-4162, and CVE-2016-4163. **Reference: CVE-2016-4160**	https://helpx.adobe.com/security/products/flash-player/apsb16-15.html	A-ADO-AIR D-80716/10
Coldfusion *ColdFusion is a commercial rapid web application development platform created by JJ Allaire in 1995.*					
Cross Site	2016-06-16	4.3	Cross-site scripting (XSS)	https://helpx	A-ADO-

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

Scripting			vulnerability in Adobe ColdFusion 10 before Update 20, 11 before Update 9, and 2016 before Update 2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-4159**	.adobe.com/security/products/coldfusion/apsb16-22.html	COLDF-80716/11
F5					
Big-ip Access Policy Manager, Big-ip Edge Gateway *F5 BIG-IP Access Policy Manager (APM) is a flexible, high-performance access and security solution that provides unified global access to your applications, network, and cloud. F5 BIG-IP Edge Gateway is an accelerated remote access solution that brings together SSL VPN, security, application acceleration, and availability services.*					
NA	2016-06-16	4	Open redirect vulnerability in F5 BIG-IP APM 11.2.1, 11.4.x, 11.5.x, and 11.6.x before 11.6.0 HF6 and Edge Gateway 11.2.1, when using multi-domain single sign-on (SSO), allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a base64-encoded URL in the SSO_ORIG_URI parameter. **Reference: CVE-2016-3687**	https://support.f5.com/kb/en-us/solutions/public/k/26/sol26738102.html	A-F5-BIG-I-80716/12
Qemu					
Qemu *QEMU (short for Quick Emulator) is a free and open-source hosted hypervisor that performs hardware virtualization. QEMU is a hosted virtual machine monitor.*					
Denial of Service; Overflow; Gain Information	2016-06-16	3.6	Multiple integer overflows in the USB Net device emulator (hw/usb/dev-network.c) in QEMU before 2.5.1 allow local guest OS administrators to cause a denial of service (QEMU process crash) or obtain sensitive host memory information via a remote NDIS control message packet that is mishandled in the (1) rndis_query_response, (2) rndis_set_response, or (3) usb_net_handle_dataout function. **Reference: CVE-2016-2538**	http://git.qemu.org/?p=qemu.git;a=commit;h=fe3c546c5ff2a6210f9a4d8561cc64051ca8603e	A-QEM-QEMU-80716/13

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

Citrix					
Ios Receiver *Citrix Receiver lets you access your enterprise files, applications, and desktops to help you be as productive on the go as you are in the office.*					
NA	2016-06-17	5.8	Citrix iOS Receiver before 7.0 allows attackers to cause TLS certificates to be incorrectly validated via unspecified vectors. **Reference: CVE-2016-5433**	http://support.citrix.com/article/CTX213998	A-CIT-IOSR-80716/14
Openstack					
Neutron *Neutron is a very simple and small time synchronizing program that retrieves the accurate time from one of several specialized time servers on the Internet.*					
Denial of Service ; Bypass	2016-06-17	6.4	The IPTables firewall in OpenStack Neutron before 7.0.4 and 8.0.0 through 8.1.0 allows remote attackers to bypass an intended MAC-spoofing protection mechanism and consequently cause a denial of service or intercept network traffic via (1) a crafted DHCP discovery message or (2) crafted non-IP traffic. **Reference: CVE-2016-5363**	http://www.openwall.com/lists/oss-security/2016/06/10/6	A-OPE-NEUTR-80716/15
Denial of Service ; Bypass	2016-06-17	6.4	The IPTables firewall in OpenStack Neutron before 7.0.4 and 8.0.0 through 8.1.0 allows remote attackers to bypass an intended DHCP-spoofing protection mechanism and consequently cause a denial of service or intercept network traffic via a crafted DHCP discovery message. **Reference: CVE-2016-5362**	http://www.openwall.com/lists/oss-security/2016/06/10/5	A-OPE-NEUTR-80716/16
Solarwinds					
Virtualization Manager *SolarWinds Virtualization Manager (VMAN) provides key monitoring and metrics for the organization.*					
Gain Privileges	2016-06-17	7.2	SolarWinds Virtualization Manager 6.3.1 and earlier allow local users to gain	http://seclists.org/fulldisclosure/2016/	A-SOL-VIRTU-80716/17

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

			privileges by leveraging a misconfiguration of sudo, as demonstrated by "sudo cat /etc/passwd." **Reference: CVE-2016-3643**	Jun/26	
Execute Code	2016-06-17	10	The RMI service in SolarWinds Virtualization Manager 6.3.1 and earlier allows remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library. **Reference: CVE-2016-3642**	http://seclists.org/fulldisclosure/2016/Jun/29	A-SOL-VIRTU-80716/18
Cisco					
Firepower Management Center *The Cisco Firepower Management Center is the administrative nerve center for a number of Cisco security products running on a number of different platforms. It provides complete and unified management of firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection.*					
Cross Site Scripting	2016-06-17	4.3	Cross-site scripting (XSS) vulnerability in Cisco Firepower Management Center 4.10.3, 5.2.0, 5.3.0, 5.3.1, and 5.4.0 allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka Bug ID CSCur25516. **Reference: CVE-2016-1431**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160617-fmc	A-CIS-FIREP-80716/19
Prime Network Registrar *Cisco Prime Network Registrar provides scalable, reliable, and integrated capabilities (DNS, DHCP, IPAM) that ease the transition to IPv6.*					
Gain Information	2016-06-17	5	The System Configuration Protocol (SCP) core messaging interface in Cisco Prime Network Registrar 8.2 before 8.2.3.1 and 8.3 before 8.3.2 allows remote attackers to obtain sensitive information via crafted SCP messages, aka Bug ID CSCuv35694. **Reference: CVE-2016-1427**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160616-pnr	A-CIS-PRIME-80716/20
Openstack					

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

Neutron *Neutron is a very simple and small time synchronizing program that retrieves the accurate time from one of several specialized time servers on the Internet.*					
Denial of Service ; Bypass	2016-06-17	6.4	The IPTables firewall in OpenStack Neutron before 7.0.4 and 8.0.0 through 8.1.0 allows remote attackers to bypass an intended ICMPv6-spoofing protection mechanism and consequently cause a denial of service or intercept network traffic via a link-local source address. **Reference: CVE-2015-8914**	http://www.openwall.com/lists/oss-security/2016/06/10/6	A-OPE-NEUTR-80716/21
Dx Library Project					
Dx Library *Project Description dx.h is a modern C++ library that aims to simplify DirectX-related development in C++.*					
Execute Code	2016-06-18	7.5	The printfDx function in Takumi Yamada DX Library for Borland C++ 3.13f through 3.16b, DX Library for Gnu C++ 3.13f through 3.16b, and DX Library for Visual C++ 3.13f through 3.16b allows remote attackers to execute arbitrary code via a crafted string. **Reference:CVE-2016-4819**	http://dxlib.o.oo7.jp/dxvulnerability.html	A-DX -DXLI-80716/22
H2o Project					
H2O *H2O is open-source software for big-data analysis. It is produced by the start-up H2O.ai (formerly 0xdata), which launched in 2011 in Silicon Valley.*					
Denial of Service ; Execute Code	2016-06-18	5	lib/http2/connection.c in H2O before 1.7.3 and 2.x before 2.0.0-beta5 mishandles HTTP/2 disconnection, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly execute arbitrary code via a crafted packet. **Reference: CVE-2016-4817**	http://jvn.jp/en/jp/JVN87859762/index.html	A-H2O-H2O-80716/23
Netcommons					
Netcommons *netCommons is a Horizon2020 research project, which proposes a novel transdisciplinary*					

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

methodology on promoting and supporting the creation of network infrastructures as commons, for resiliency, sustainability, democracy, self-determination, and social integration.					
Gain Privileges	2016-06-18	9	NetCommons 2.4.2.1 and earlier allows remote authenticated secretariat (aka CLERK) users to gain privileges by creating a SYSTEM_ADMIN account. **Reference:CVE-2016-4813**	http://jvndb.jvn.jp/jvndb/JVNDB-2016-000075	A-NET-NETCO-80716/24
Trend Micro					
Business Security, Business Security Services *Trend Micro Worry-Free Services provides enterprise-class protection for Windows, Mac, and mobile devices from a secure, centralized, web-based management console.*					
Cross Site Scripting	2016-06-18	4.3	CRLF injection vulnerability in Trend Micro Worry-Free Business Security Service 5.x and Worry-Free Business Security 9.0 allows remote attackers to inject arbitrary HTTP headers and conduct cross-site scripting (XSS) attacks via unspecified vectors. **Reference: CVE-2016-1224**	http://jvndb.jvn.jp/jvndb/JVNDB-2016-000089	A-TRE-BUSIN-80716/25
Directory traversal	2016-06-18	5	Directory traversal vulnerability in Trend Micro Office Scan 11.0, Worry-Free Business Security Service 5.x, and Worry-Free Business Security 9.0 allows remote attackers to read arbitrary files via unspecified vectors. **Reference: CVE-2016-1223**	http://esupport.trendmicro.com/solution/ja-JP/1114102.aspx	A-TRE-BUSIN-80716/26
Nttdata					
Bypass	2016-06-18	4.3	NTT Data TERASOLUNA Server Framework for Java(WEB) 2.0.0.1 through 2.0.6.1, as used in Fujitsu Interstage Business Application Server and other products, allows remote attackers to bypass a file-extension protection mechanism, and consequently read arbitrary files, via a crafted pathname.	http://jvn.jp/en/jp/JVN74659077/index.html	A-NTT-TERAS-80716/27

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

			Reference:CVE-2016-1183		
Ntt-bp					
Japan Connected-free Wi-fi *Japan Connected-free Wi-Fi (Japan Wi-Fi) is a new application for iPhone and Android that enables users to connect to free, fast and reliable Wi-Fi at the touch of a button.*					
NA	2016-06-19	5.1	The NTT Broadband Platform Japan Connected-free Wi-Fi application 1.15.1 and earlier for Android and 1.13.0 and earlier for iOS allows man-in-the-middle attackers to obtain API access via unspecified vectors. **Reference: CVE-2016-4811**	http://jvn.jp/en/jp/JVN46888319/278948/index.html	A-NTT-JAPAN-80716/28
Osisoft					
Pi Af Server 2016 *OSIsoft PI AF Server before 2016 2.8.0 allows remote authenticated users to cause a denial of service (service outage) via a message.*					
Denial of Service	2016-06-19	4	OSIsoft PI AF Server before 2016 2.8.0 allows remote authenticated users to cause a denial of service (service outage) via a message. **Reference: CVE-2016-4518**	https://techsupport.osisoft.com/Troubleshooting/Alerts/AL00301	A-OSI-PI AF-80716/29
Fonality					
Fonality, Hud Web *Fonality's PBXtra is the largest distributed deployment of Asterisk, with more than 10000 users having placed more than 20 million calls. Heads Up Display (HUD) system allows businesses to easily and effectively collaborate across one unified communication tool.*					
NA	2016-06-19	5	The Chrome HUDweb plugin before 2016-05-05 for Fonality (previously trixbox Pro) 12.6 through 14.1i uses the same hardcoded private key across different customers' installations, which allows remote attackers to defeat cryptographic protection mechanisms by leveraging knowledge of this key from another installation. **Reference:CVE-2016-2364**	http://www.kb.cert.org/vuls/id/754056	A-FON-FONAL-80716/30
Execute Code	2016-06-19	7.2	Fonality (previously trixbox Pro) 12.6 through 14.1i before 2016-06-01 uses weak permissions for the	http://www.kb.cert.org/vuls/id/754056	A-FON-FONAL-80716/31

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

			/var/www/rpc/surun script, which allows local users to obtain root access for unspecified command execution by leveraging access to the nobody account. **Reference:CVE-2016-2363**		
NA	2016-06-19	10	Fonality (previously trixbox Pro) 12.6 through 14.1i before 2016-06-01 has a hardcoded password for the FTP account, which allows remote attackers to obtain access via a (1) FTP or (2) SSH connection. **Reference: CVE-2016-2362**	http://www.kb.cert.org/vuls/id/754056	A-FON-FONAL-80716/32
Openssl					
Openssl *In computer networking, OpenSSL is a software library to be used in applications that need to secure communications against eavesdropping or need to ascertain the identity of the party at the other end. It has found wide use in internet web servers, serving a majority of all web sites.*					
Gain Information	2016-06-19	2.1	The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack. **Reference: CVE-2016-2178**	http://eprint.iacr.org/2016/594.pdf	A-OPE-OPENS-80716/33
Denial of Service ; Overflow	2016-06-19	7.5	OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.	https://bugzilla.redhat.com/show_bug.cgi?id=1341705	A-OPE-OPENS-80716/34

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

			Reference: CVE-2016-2177		
Trendmicro					
Internet Security *Internet security is a branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole.*					
Cross Site Scripting	2016-06-19	4.3	Cross-site scripting (XSS) vulnerability in Trend Micro Internet Security 8 and 10 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-1226**	https://esupport.trendmicro.com/support/vb/solution/ja-jp/1113880.aspx	A-TRE-INTER-80716/35
Gain Information	2016-06-19	5	Trend Micro Internet Security 8 and 10 allows remote attackers to read arbitrary files via unspecified vectors. **Reference: CVE-2016-1225**	http://jvn.jp/en/jp/JVN48789425/index.html	A-TRE-INTER-80716/36
Cybozu					
Garoon *Fujitsu and Cybozu, Inc. jointly announced that they have reached an agreement to collaborate on providing Cybozu Garoon, Cybozu's enterprise groupware product, under the Software-as-a-Service (SaaS) model.*					
Cross Site Scripting	2016-06-19	4.3	Cross-site scripting (XSS) vulnerability in Cybozu Garoon 4.x before 4.2.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2015-7775. **Reference: CVE-2016-1197**	https://support.cybozu.com/ja-jp/article/9303	A-CYB-GAROO-80716/37
Bypass ;Gain Information	2016-06-19	4	Cybozu Garoon 3.x and 4.x before 4.2.1 allows remote authenticated users to bypass intended access restrictions and obtain sensitive Address Book information via an API call, a different vulnerability than	http://jvn.jp/en/jp/JVN33879831/index.html	A-CYB-GAROO-80716/38

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

			CVE-2015-7776. **Reference:CVE-2016-1196**		
NA	2016-06-19	5.8	Open redirect vulnerability in Cybozu Garoon 3.x and 4.x before 4.2.1 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a crafted URL. **Reference: CVE-2016-1195**	https://support.cybozu.com/ja-jp/article/8987	A-CYB-GAROO-80716/39
Directory Traversal	2016-06-19	4	Directory Traversal vulnerability in the logging implementation in Cybozu Garoon 3.7 through 4.2 allows remote authenticated users to read a log file via unspecified vectors. **Reference: CVE-2016-1192**	http://jvn.jp/en/jp/JVN14749391/index.html	A-CYB-GAROO-80716/40
Directory Traversal	2016-06-19	5	Directory traversal vulnerability in the Files function in Cybozu Garoon 3.x and 4.x before 4.2.1 allows remote attackers to modify settings via unspecified vectors. **Reference: CVE-2016-1191**	http://jvn.jp/en/jp/JVN14749391/index.html	A-CYB-GAROO-80716/41
IBM					
Elastic Storage Server, General Parallel File System Storage Server *The IBM Elastic Storage Server offering combines the CPU and I/O capability of the IBM POWER8 architecture matched with IBM System Storage assets. GPFS is among the leading file systems for high performance computing (HPC) applications. Storage used for large supercomputers is often GPFS-based, and GPFS is also popular for commercial applications requiring high-speed access to large volumes of data, such as digital media, seismic data processing and engineering design.*					
Gain Privileges	2016-06-19	4.6	IBM General Parallel File System (GPFS) in GPFS Storage Server 2.0.0 through 2.0.7 and Elastic Storage Server 2.5.x through 2.5.5, 3.x before 3.5.5, and 4.x before 4.0.3, as distributed in Spectrum Scale RAID, allows local users to gain privileges via a crafted parameter to a setuid program.	http://www-01.ibm.com/support/docview.wss?uid=swg1IV84206	A-IBM-ELAST-80716/42

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

			Reference: CVE-2016-0392		
Cybozu					
Garoon *Fujitsu and Cybozu, Inc. jointly announced that they have reached an agreement to collaborate on providing Cybozu Garoon, Cybozu's enterprise groupware product, under the Software-as-a-Service (SaaS) model.*					
Gain Information	2016-06-19	4.3	Cybozu Garoon 3.x and 4.x before 4.2.0 does not properly restrict loading of IMG elements, which makes it easier for remote attackers to track users via a crafted HTML e-mail message, a different vulnerability than CVE-2016-1196. **Reference: CVE-2015-7776**	http://jvn.jp/en/jp/JVN53542912/index.html	A-CYB-GAROO-80716/43
Cross Site Scripting	2016-06-19	3.5	Cross-site scripting (XSS) vulnerability in Cybozu Garoon 4.0.3 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2016-1197. **Reference: CVE-2015-7775**	https://support.cybozu.com/ja-jp/article/8893	A-CYB-GAROO-80716/44
IBM					
Websphere Mq *Websphere MQ, formerly known as MQ (message queue) series, is an IBM standard for program-to-program messaging across multiple platforms. Websphere MQ is sometimes referred to as message-oriented middleware (MOM).*					
NA	2016-06-19	2.1	IBM WebSphere MQ 8.0.0.4 on IBM i platforms allows local users to discover cleartext certificate-keystore passwords within MQ trace output by leveraging administrator privileges to execute the mqcertck program. **Reference: CVE-2015-7462**	http://www-01.ibm.com/support/docview.wss?uid=swg21984557	A-IBM-WEBSP-80716/45
Cisco					
Unified Contact Center Enterprise *Cisco Unified Contact Center Enterprise delivers intelligent contact routing, call treatment, network-to-desktop computer telephony integration (CTI), and multichannel contact management over an IP infrastructure.*					
Cross Site Scripting	2016-06-22	4.3	Cross-site scripting (XSS) vulnerability in the management interface in	http://tools.cisco.com/security/cente	A-CIS-UNIFI-80716/46

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

			Cisco Unified Contact Center Enterprise through 10.5(2) allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka Bug ID CSCux59650. **Reference: CVE-2016-1439**	r/content/CiscoSecurityAdvisory/cisco-sa-20160622-ucce	
Cisco					
Prime Collaboration Deployment *Cisco Prime Collaboration Deployment allows a user to perform tasks (such as migration or upgrade) on servers that are in the inventory.*					
Execute Code; Structured Query Language	2016-06-22	4	SQL injection vulnerability in the SQL database in Cisco Prime Collaboration Deployment before 11.5.1 allows remote authenticated users to execute arbitrary SQL commands via a crafted URL, aka Bug ID CSCuy92549. **Reference: CVE-2016-1437**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160621-pcd	A-CIS-PRIME-80716/47
Asr 5000 Software *The Cisco ASR 5000 Series combines massive performance and scale with flexibility, virtualization, and intelligence—so network resources are available exactly when they are needed.*					
Denial of Service; Overflow	2016-06-22	5	The General Packet Radio Switching Tunneling Protocol 1 (aka GTPv1) implementation on Cisco ASR 5000 Packet Data Network Gateway devices before 19.4 allows remote attackers to cause a denial of service (Session Manager process restart) via a crafted GTPv1 packet, aka Bug ID CSCuz46198. **Reference: CVE-2016-1436**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160621-asr	A-CIS-ASR5-80716/48
EMC					
Documentum Administrator, Documentum Capital Projects; Documentum Taskspace; Documentum Webtop *Documentum is an enterprise content management platform, now owned by EMC Corporation, as well as the name of the software company that originally developed the technology. EMC acquired Documentum for $1.7 billion in December, 2003.The Documentum platform is part of EMC's Enterprise Content Division (ECD) business unit, one of EMC's four operating divisions.*					
Execute Code; Bypass	2016-06-22	6.5	EMC Documentum WebTop 6.8 before Patch 13 and 6.8.1 before Patch 02, Documentum Administrator 7.x before 7.2	http://seclists.org/bugtraq/2016/Jun/92	A-EMC-DOCUM-80716/49

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

			Patch 13, Documentum Capital Projects 1.9 before Patch 23 and 1.10 before Patch 10, and Documentum TaskSpace 6.7 SP3 allow remote authenticated users to bypass intended access restrictions and execute arbitrary IAPI/IDQL commands via the IAPI/IDQL interface. **Reference: CVE-2016-0914**		
Huawei					
Fusioninsight Hd *Huawei FusionInsight HD allows local users to gain root privileges via unspecified vectors.*					
Gain Privileges	2016-06-24	7.2	Huawei FusionInsight HD before V100R002C60SPC200 allows local users to gain root privileges via unspecified vectors. **Reference: CVE-2016-5723**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160617-01-fusioninsight-en	A-HUA-FUSIO-80716/50
Ocean Stor Firmware *Huawei's OceanStor high-end storage systems feature advanced hardware, software, multiple converged storage for large file sharing, and cloud computing.*					
Gain Information	2016-06-24	7.5	OceanStor 5300 V3, 5500 V3, 5600 V3, 5800 V3, 6800 V3, 18800 V3, and 18500 V3 before V300R003C10 sends the plaintext session token in the HTTP header, which allows remote attackers to conduct replay attacks and obtain sensitive information by sniffing the network. **Reference: CVE-2016-5722**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160615-01-oceanstor-en	A-HUA-OCEAN-80716/51
Solarwinds					
Virtualization Manager *SolarWinds Virtualization Manager (VMAN) provides key monitoring and metrics for the organization*					
Gain Information	2016-06-24	1.9	SolarWinds Virtualization Manager 6.3.1 and earlier uses weak encryption to store passwords in /etc/shadow,	http://seclists.org/fulldisclosure/2016/Jun/38	A-SOL-VIRTU-80716/52

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

			which allows local users with superuser privileges to obtain user passwords via a brute force attack. **Reference: CVE-2016-5709**		
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 Domain Name System; Big-ip Link Controller; Big-ip Local Traffic Manager; Big-ip Policy Enforcement Manager; Big-iq Cloud; Big-iq Cloud And Orchestration; Big-iq Device; Big-iq Security *The BIG-IP family of products offers the application intelligence that network managers need to ensure applications are fast, secure, and available. BIG-IQ Centralized Management provides single pane-of-glass management of your physical and virtual BIG-IP devices.*					
Gain Information	2016-06-24	4	The iControl REST service in F5 BIG-IP LTM, AAM, AFM, Analytics, APM, ASM, Link Controller, and PEM 11.5.x before 11.5.4, 11.6.x before 11.6.1, and 12.x before 12.0.0 HF3; BIG-IP DNS 12.x before 12.0.0 HF3; BIG-IP GTM 11.5.x before 11.5.4 and 11.6.x before 11.6.1; BIG-IQ Cloud and Security 4.0.0 through 4.5.0; BIG-IQ Device 4.2.0 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 remote authenticated administrators to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-5021**	https://support.f5.com/kb/en-us/solutions/public/k/99/sol99998454/	A-F5-BIG-I-80716/53
Haxx					
Curl *cURL is a computer software project providing a library and command-line tool for transferring data using various protocols*					
Execute Code	2016-06-24	6.9	Multiple untrusted search path vulnerabilities in cURL and libcurl before 7.49.1, when built with SSPI or telnet is enabled, allow local users to execute arbitrary code and conduct DLL hijacking attacks	https://curl.haxx.se/docs/adv_20160530.html	A-HAX-CURL-80716/54

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

			via a Trojan horse (1) security.dll, (2) secur32.dll, or (3) ws2_32.dll in the application or current working directory. **Reference: CVE-2016-4802**		
Advantech					
Webaccess *Web Access is an enterprise business solutions provider for SMEs and an open source solutions provider for non-profits.*					
Denial of Service; Overflow	2016-06-24	4.3	Buffer overflow in Advantech WebAccess before 8.1_20160519 allows local users to cause a denial of service via a crafted DLL file. **Reference: CVE-2016-4528**	https://ics-cert.us-cert.gov/advisories/ICSA-16-173-01	A-ADV-WEBAC-80716/55
Gain Information	2016-06-24	3.3	Unspecified ActiveX controls in Advantech WebAccess before 8.1_20160519 allow remote authenticated users to obtain sensitive information or modify data via unknown vectors, related to the INTERFACESAFE_FOR_UNTRUSTED_CALLER (aka safe for scripting) flag. **Reference: CVE-2016-4525**	https://ics-cert.us-cert.gov/advisories/ICSA-16-173-01	A-ADV-WEBAC-80716/56
Unitronics					
Visilogic Oplc Ide *Unitronics VisiLogic OPLC IDE before 9.8.02 allows remote attackers to execute unspecified code via unknown vectors.*					
Execute Code; Overflow	2016-06-24	7.5	Stack-based buffer overflow in Unitronics VisiLogic OPLC IDE before 9.8.30 allows remote attackers to execute arbitrary code via a crafted filename field in a ZIP archive in a vlp file. **Reference: CVE-2016-4519**	https://ics-cert.us-cert.gov/advisories/ICSA-16-175-02	A-UNI-VISIL-80716/57
Alertus					
Alertus Desktop Notification For Os X *Alertus Desktop uses xMatters to deliver important notifications to relevant people on the channel and device they prefer.*					
NA	2016-06-25	3.6	Alertus Desktop Notification before 2.9.31.1710 on OS X uses weak permissions for configuration files and	http://www.kb.cert.org/vuls/id/BLUU-A9TJHR	A-ALE-ALERT-80716/58

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

			unspecified other files, which allows local users to suppress emergency notifications or change content via standard filesystem operations. **Reference: CVE-2016-5087**		
Welcart					
E-commerce *Welcart e-Commerce assists you to build online shop system.*					
NA	2016-06-25	6.4	The Collne Welcart e-Commerce plugin before 1.8.3 for WordPress mishandles sessions, which allows remote attackers to obtain access by leveraging knowledge of the e-mail address associated with an account. **Reference: CVE-2016-4828**	http://jvn.jp/en/jp/JVN61578437/index.html	A-WEL-E-COM-80716/59
Cross Site Scripting	2016-06-25	4.3	Cross-site scripting (XSS) vulnerability in the Collne Welcart e-Commerce plugin before 1.8.3 for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2016-4826. **Reference: CVE-2016-4827**	http://jvndb.jvn.jp/jvndb/JVNDB-2016-000117	A-WEL-E-COM-80716/60
Cross Site Scripting	2016-06-25	4.3	Cross-site scripting (XSS) vulnerability in the Collne Welcart e-Commerce plugin before 1.8.3 for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2016-4827. **Reference: CVE-2016-4826**	http://www.welcart.com/community/archives/78977	A-WEL-E-COM-80716/61
Execute Code	2016-06-25	6.8	The Collne Welcart e-Commerce plugin before 1.8.3 for WordPress allows remote attackers to conduct PHP object injection attacks and execute arbitrary PHP code via crafted serialized data.	http://www.welcart.com/community/archives/78977	A-WEL-E-COM-80716/62

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

			Reference: CVE-2016-4825		
IBM					
Web Content Manager; Websphere Portal *IBM Web Content Manager is designed to accelerate digital content development and deployment through all your digital channels. IBM WebSphere Portal products provide enterprise web portals that help companies deliver a highly-personalized, social experience for their customers.*					
Cross Site Scripting; Cross Site Request Forgery	2016-06-25	6.8	Cross-site request forgery (CSRF) vulnerability in the PA_Theme_Creator application in IBM WebSphere Portal 8.5 CF08 through CF10 and Web Content Manager allows remote attackers to hijack the authentication of arbitrary users for requests that insert XSS sequences. **Reference: CVE-2016-2901**	http://www-01.ibm.com/support/docview.wss?uid=swg1PI62594	A-IBM-WEB C-80716/63
Cybozu					
Garoon *Fujitsu and Cybozu, Inc. jointly announced that they have reached an agreement to collaborate on providing Cybozu Garoon, Cybozu's enterprise groupware product, under the Software-as-a-Service (SaaS) model.*					
Gain Information	2016-06-25	5	Cybozu Garoon 3.7 through 4.2 allows remote attackers to obtain sensitive email-reading information via unspecified vectors. **Reference: CVE-2016-1193**	http://jvn.jp/en/jp/JVN25765762/index.html	A-CYB-GAROO-80716/64
Bypass	2016-06-25	4	Cybozu Garoon 3.1 through 4.2 allows remote authenticated users to bypass intended restrictions on MultiReport reading via unspecified vectors. **Reference: CVE-2016-1190**	http://jvn.jp/en/jp/JVN18975349/index.html	A-CYB-GAROO-80716/65
Bypass	2016-06-25	5.5	Cybozu Garoon 3.x and 4.x before 4.2.1 allows remote authenticated users to bypass intended restrictions on reading, creating, or modifying a portlet via unspecified vectors. **Reference: CVE-2016-1189**	http://jvndb.jvn.jp/jvndb/JVNDB-2016-000093	A-CYB-GAROO-80716/66
NA	2016-06-25	4	Cybozu Garoon 3.x and 4.x before 4.2.1 allows remote	http://jvndb.jvn.jp/jvndb/	A-CYB-GAROO-

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

			authenticated users to send spoofed e-mail messages via unspecified vectors. **Reference: CVE-2016-1188**	JVNDB-2016-000077	80716/67
IBM					
Domino *IBM Domino (formerly IBM Lotus Domino) is an advanced platform for hosting social business applications.*					
Execute Code ; Overflow	2016-06-26	6.8	Heap-based buffer overflow in the KeyView PDF filter in IBM Domino 8.5.x before 8.5.3 FP6 IF13 and 9.x before 9.0.1 FP6 allows remote attackers to execute arbitrary code via a crafted PDF document, a different vulnerability than CVE-2016-0277, CVE-2016-0278, and CVE-2016-0279. **Reference: CVE-2016-0301**	http://www-01.ibm.com/support/docview.wss?uid=swg21983292	A-IBM-DOMIN-80716/68
Execute Code ; Overflow	2016-06-26	6.8	Heap-based buffer overflow in the KeyView PDF filter in IBM Domino 8.5.x before 8.5.3 FP6 IF13 and 9.x before 9.0.1 FP6 allows remote attackers to execute arbitrary code via a crafted PDF document, a different vulnerability than CVE-2016-0277, CVE-2016-0278, and CVE-2016-0301. **Reference: CVE-2016-0279**	http://www-01.ibm.com/support/docview.wss?uid=swg21983292	A-IBM-DOMIN-80716/69
Execute Code; Overflow	2016-06-26	6.8	Heap-based buffer overflow in the KeyView PDF filter in IBM Domino 8.5.x before 8.5.3 FP6 IF13 and 9.x before 9.0.1 FP6 allows remote attackers to execute arbitrary code via a crafted PDF document, a different vulnerability than CVE-2016-0277, CVE-2016-0279, and CVE-2016-0301. **Reference:CVE-2016-0278**	http://www-01.ibm.com/support/docview.wss?uid=swg21983292	A-IBM-DOMIN-80716/70
Execute Code; Overflow	2016-06-26	6.8	Heap-based buffer overflow in the KeyView PDF filter in IBM Domino 8.5.x before 8.5.3 FP6 IF13 and 9.x before 9.0.1 FP6 allows remote attackers to execute arbitrary code via a	http://www-01.ibm.com/support/docview.wss?uid=swg21983292	A-IBM-DOMIN-80716/71

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

			crafted PDF document, a different vulnerability than CVE-2016-0278, CVE-2016-0279, and CVE-2016-0301. **Reference: CVE-2016-0277**		
Websphere Mq *IBM WebSphere Portal products provide enterprise web portals that help companies deliver a highly-personalized, social experience for their customers.*					
Bypass; Gain Information	2016-06-26	2.1	runmqsc in IBM WebSphere MQ 8.x before 8.0.0.5 allows local users to bypass an intended +dsp authority requirement and obtain sensitive information via unspecified display commands. **Reference: CVE-2016-0259**	http://www-01.ibm.com/support/docview.wss?uid=swg21984561	A-IBM-WEBSP-80716/72
Bypass	2016-06-26	2.1	runmqsc in IBM WebSphere MQ 8.x before 8.0.0.5 allows local users to bypass intended queue-manager command access restrictions by leveraging authority for +connect and +dsp. **Reference: CVE-2015-7473**	http://www-01.ibm.com/support/docview.wss?uid=swg21984555	A-IBM-WEBSP-80716/73
IBM					
Marketing Platform *IBM Marketing Platform provides security, configuration, notification, and dashboard features for IBMEMM products.*					
Execute Code; Structured Query Language	2016-06-27	6.5	SQL injection vulnerability in IBM Marketing Platform 8.5.x, 8.6.x, and 9.x before 9.1.2.2 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors. **Reference: CVE-2016-0233**	http://www-01.ibm.com/support/docview.wss?uid=swg21980989	A-IBM-MARKE-80716/74
Cross Site Scripting	2016-06-27	4.3	Cross-site scripting (XSS) vulnerability in IBM Marketing Platform 8.6.x and 9.x before 9.1.2.2 allows remote attackers to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-0229**	http://www-01.ibm.com/support/docview.wss?uid=swg21980989	A-IBM-MARKE-80716/75
Execute Code Structured Query	2016-06-27	7.5	SQL injection vulnerability in	http://www-01.ibm.com/	A-IBM-MARKE-

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

Language			IBM Marketing Platform 8.5.x, 8.6.x, and 9.x before 9.1.2.2 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. **Reference: CVE-2016-0224**	support/docview.wss?uid=swg21980989	80716/76
IBM					
Domino *IBM Domino (formerly IBM Lotus Domino) is an advanced platform for hosting social business applications.*					
Execute Code; Bypass	2016-06-28	6.8	The Java Console in IBM Domino 8.5.x before 8.5.3 FP6 IF13 and 9.x before 9.0.1 FP6, when a certain unsupported configuration involving UNC share pathnames is used, allows remote attackers to bypass authentication and possibly execute arbitrary code via unspecified vectors, aka SPR KLYHA7MM3J. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-0920. **Reference: CVE-2016-0304**	http://www-01.ibm.com/support/docview.wss?uid=swg21983328	A-IBM-DOMIN-80716/77
Security Guardium *IBM Security Guardium is a comprehensive data security platform that provides a full range of capabilities – from discovery and classification of sensitive data to vulnerability assessment to data and file activity monitoring to masking, encryption, blocking, alerting and quarantining to protect sensitive data.*					
Directory traversal ; Gain Information	2016-06-28	4	Directory traversal vulnerability in IBM Security Guardium Database Activity Monitor 10 before 10.0p100 allows remote authenticated users to read arbitrary files via a crafted URL. **Reference: CVE-2016-0298**	http://www-01.ibm.com/support/docview.wss?uid=swg21981749	A-IBM-SECUR-80716/78
Urbancode Deploy *IBM UrbanCode Deploy is a tool for automating application deployments through your environments.*					
Gain Information	2016-06-28	4	IBM UrbanCode Deploy 6.0.x before 6.0.1.13, 6.1.x before 6.1.3.3, and 6.2.x before 6.2.1.1 allows remote	http://www-01.ibm.com/support/docview.wss?	A-IBM-URBAN-80716/79

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

			authenticated users to obtain sensitive cleartext secure-property information via (1) the server UI or (2) a database request. **Reference: CVE-2016-0267**	uid=swg2C1000151	
Wordpress					
Wordpress *WordPress is web software you can use to create a beautiful website, blog, or app.*					
Bypass	2016-06-29	5	WordPress before 4.5.3 allows remote attackers to bypass the sanitize_file_name protection mechanism via unspecified vectors. **Reference: CVE-2016-5839**	https://codex.wordpress.org/Version_4.5.3	A-WOR-WORDP-80716/84
Bypass	2016-06-29	5	WordPress before 4.5.3 allows remote attackers to bypass intended password-change restrictions by leveraging knowledge of a cookie. **Reference: CVE-2016-5838**	https://wordpress.org/news/2016/06/wordpress-4-5-3/	A-WOR-WORDP-80716/85
Bypass	2016-06-29	5	WordPress before 4.5.3 allows remote attackers to bypass intended access restrictions and remove a category attribute from a post via unspecified vectors. **Reference: CVE-2016-5837**	https://wordpress.org/news/2016/06/wordpress-4-5-3/	A-WOR-WORDP-80716/86
Denial of Service	2016-06-29	5	The oEmbed protocol implementation in WordPress before 4.5.3 allows remote attackers to cause a denial of service via unspecified vectors. **Reference: CVE-2016-5836**	https://wordpress.org/news/2016/06/wordpress-4-5-3/	A-WOR-WORDP-80716/87
Gain Information	2016-06-29	5	WordPress before 4.5.3 allows remote attackers to obtain sensitive revision-history information by leveraging the ability to read a post, related to wp-admin/includes/ajax-actions.php and wp-admin/revision.php. **Reference: CVE-2016-5835**	https://wordpress.org/news/2016/06/wordpress-4-5-3/	A-WOR-WORDP-80716/88
Cross-site scripting	2016-06-29	4.3	Cross-site scripting (XSS) vulnerability in the wp_get_attachment_link	https://github.com/WordPress/WordP	A-WOR-WORDP-80716/89

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

			function in wp-includes/post-template.php in WordPress before 4.5.3 allows remote attackers to inject arbitrary web script or HTML via a crafted attachment name, a different vulnerability than CVE-2016-5833. **Reference: CVE-2016-5834**	ress/commit/4372cdf45d0f49c74bbd4d60db7281de83e32648	
Cross-site scripting	2016-06-29	4.3	Cross-site scripting (XSS) vulnerability in the column_title function in wp-admin/includes/class-wp-media-list-table.php in WordPress before 4.5.3 allows remote attackers to inject arbitrary web script or HTML via a crafted attachment name, a different vulnerability than CVE-2016-5834. **Reference: CVE-2016-5833**	https://github.com/WordPress/WordPress/commit/4372cdf45d0f49c74bbd4d60db7281de83e32648	A-WOR-WORDP-80716/90
Bypass	2016-06-29	5	The customizer in WordPress before 4.5.3 allows remote attackers to bypass intended redirection restrictions via unspecified vectors. **Reference: CVE-2016-5832**	https://codex.wordpress.org/Version_4.5.3	A-WOR-WORDP-80716/91
Opera					
Opera Mail *Opera Mail (formerly known as M2) is the email and news client developed by Opera Software.*					
Execute Code	2016-06-29	9.3	Unspecified vulnerability in Opera Mail before 2016-02-16 on Windows allows user-assisted remote attackers to execute arbitrary code via a crafted e-mail message. **Reference: CVE-2016-5101**	http://www.opera.com/blogs/security/2016/02/opera-12-and-opera-mail-security-update/	A-OPE-OPERA-80716/92
HP					
Service Manager, Service Manager Mobility, Service Manager Server, Service Manager Service Request Catalog, Service Manager Web Client, Service Manager Windows Client *The HP Service Manager is one of the applications acquired by HP when it purchased Peregrine Systems in 2005. The application was originally known as PNMS (Peregrine Network Management System). After releasing the first version of PNMS, Peregrine Systems eventually added functionality such as Request Management, Call Management, and Change Management and rebranded the application as Peregrine Service Center.*					
Gain Information	2016-06-18	6	HP Service Manager Software	https://h205	A-HP-

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

			9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, and 9.41 allows remote authenticated users to obtain sensitive information, modify data, and conduct server-side request forgery (SSRF) attacks via unspecified vectors, related to the Server, Web Client, Windows Client, and Service Request components. **Reference:CVE-2016-4371**	66.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05167176	SERVI-80716/93
Application /Operating System (A/OS)					
Debian/Libexpat					
Debian Linux/Expat: *Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals called the Debian Project. In computing, Expat is a stream-oriented XML 1.0 parser library, written in C.*					
Denial of Service	2016-06-16	7.8	The XML parser in Expat does not use sufficient entropy for hash initialization, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted identifiers in an XML document. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-0876. **Reference: CVE-2016-5300**	NA	O-DEB-DEBIA-80716/94
Adobe/Microsoft					
Creative Cloud/Windows *Adobe Creative Cloud is a software as a service offering from Adobe Systems that gives users access to a collection of software developed by Adobe for graphic design, video editing, web development, photography, andcloud services. Microsoft Windows (commonly Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft*					
Gain Privileges	2016-06-16	6.9	Unquoted Windows search path vulnerability in Adobe Creative Cloud Desktop Application before 3.7.0.272 on Windows allows local users to gain privileges via a Trojan horse executable file in the %SYSTEMDRIVE% directory. **Reference: CVE-2016-4158**	https://helpx.adobe.com/security/products/creative-cloud/apsb16-21.html	A-ADO-CREAT-80716/95
Adobe					

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

Creative Cloud *Adobe Creative Cloud is a software as a service offering from Adobe Systems that gives users access to a collection of software developed by Adobe for graphic design, video editing, web development, photography, andcloud services*					
Gain privileges	2016-06-16	6.9	Untrusted search path vulnerability in the installer in Adobe Creative Cloud Desktop Application before 3.7.0.272 on Windows allows local users to gain privileges via a Trojan horse resource in an unspecified directory. **Reference: CVE-2016-4157**	https://helpx.adobe.com/security/products/creative-cloud/apsb16-21.html	A-ADO-CREAT-80716/96
Flash Player;Flash Player For Linux *Adobe Flash Player is the high performance, lightweight, highly expressive client runtime that delivers powerful and consistent user experiences across major operating systems, browsers, mobile phones and devices.*					
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4156**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/97
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4155**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/98
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/99

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

			vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4154**		
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4153**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/100
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4152**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/101
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4151**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/102
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/103

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

			Reference: CVE-2016-4150		
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4149**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/104
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4148**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/105
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4147**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/106
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4146**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/107
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242	http://technet.microsoft.	A-ADO-FLASH-

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

			and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4145**	com/en-us/security/bulletin/ms16-083	80716/108
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4144**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/109
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4143**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/110
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4142**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/111
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge,	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/112

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

			has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4141**		
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4140**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/113
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4139**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/114
NA	2016-06-16	10	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4138**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/115
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/116

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

			Reference: CVE-2016-4137		
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4136**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/117
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4135**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/118
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4134**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/119
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4133**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/120
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242	http://technet.microsoft.	A-ADO-FLASH-

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

			and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4132**	com/en-us/security/bulletin/ms16-083	80716/121
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4131**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/122
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4130**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/123
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4129**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/124
NA	2016-06-16	10	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge,	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/125

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

			has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4128**		
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4127**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/126
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4126**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/127
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4125**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/128
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/129

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

			attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4124**		
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4123**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/130
NA	2016-06-16	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083. **Reference: CVE-2016-4122**	http://technet.microsoft.com/en-us/security/bulletin/ms16-083	A-ADO-FLASH-80716/131
Air Desktop Runtime, Air Sdk, Air Sdk and Compiler, Flash Player *Adobe AIR (Adobe Integrated Runtime) is a developer's tool for creating platform-independent web applications that can be run on a user's desktop. The Adobe AIR SDK provides the tools necessary to build and deploy Adobe AIR applications. Adobe AIR SDK & Compiler provides developers with a consistent and flexible development environment for the delivery of out-of-browser applications and games across devices and platforms (Windows, Mac, iOS, Android). Adobe Flash Player is the high performance, lightweight, highly expressive client runtime that delivers powerful and consistent user experiences across major operating systems, browsers, mobile phones and devices.*					
Execute Code	2016-06-16	7.5	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code via unspecified vectors,	https://helpx.adobe.com/security/products/flash-player/apsb16-15.html	A-ADO-AIR D-80716/132

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

			a different vulnerability than CVE-2016-1097, CVE-2016-1106, CVE-2016-1107, CVE-2016-1108, CVE-2016-1109, CVE-2016-1110, CVE-2016-4108, and CVE-2016-4110. **Reference: CVE-2016-4121**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-06-16	7.5	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4160, CVE-2016-4161, CVE-2016-4162, and CVE-2016-4163. **Reference: CVE-2016-4120**	https://helpx.adobe.com/security/products/flash-player/apsb16-15.html	A-ADO-AIR D-80716/133
Debian, Ffmpeg, Libav					
Debian, Ffmpeg, Libav *Debian is an operating system and a distribution of Free Software. FFmpeg/Libav is a suite of open source software in command line that permits managing of audio or video streams. With FFmpeg/Libav, you can make recordings, corrections with filters, or transcode media from one format to an other. Libav is a fork of FFmpeg that can be found in the Debian repositories. If you want to use ffmpeg, you will need to change the word "avconv" to "ffmpeg" in the different commands lines.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-06-16	6.8	The mov_read_dref function in libavformat/mov.c in Libav before 11.7 and FFmpeg before 0.11 allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via the entries value in a dref box in an MP4 file. **Reference: CVE-2016-3062**	http://www.debian.org/security/2016/dsa-3603	O-DEB-DEBIA-80716/134
Canonical, Qemu					

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

Ubuntu Linux, Qemu *Ubuntu is a Debian-based Linux operating system and distribution for personal computers, smartphones and network servers. QEMU (short for Quick Emulator) is a free and open-source hosted hypervisor that performs hardware virtualization QEMU is a hosted virtual machine monitor.*					
Denial of Service	2016-06-16	2.1	The ne2000_receive function in the NE2000 NIC emulation support (hw/net/ne2000.c) in QEMU before 2.5.1 allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via crafted values for the PSTART and PSTOP registers, involving ring buffer control. **Reference: CVE-2016-2841**	https://bugzilla.redhat.com/show_bug.cgi?id=1303106	O-CAN-UBUNT-80716/135
Denial of Service	2016-06-16	2.1	The is_rndis function in the USB Net device emulator (hw/usb/dev-network.c) in QEMU before 2.5.1 does not properly validate USB configuration descriptor objects, which allows local guest OS administrators to cause a denial of service (NULL pointer dereference and QEMU process crash) via vectors involving a remote NDIS control message packet. **Reference: CVE-2016-2392**	https://lists.gnu.org/archive/html/qemu-devel/2016-02/msg02553.html	O-CAN-UBUNT-80716/136
Denial of Service	2016-06-16	2.1	The ohci_bus_start function in the USB OHCI emulation support (hw/usb/hcd-ohci.c) in QEMU allows local guest OS administrators to cause a denial of service (NULL pointer dereference and QEMU process crash) via vectors related to multiple eof_timers. **Reference: CVE-2016-2391**	https://lists.gnu.org/archive/html/qemu-devel/2016-02/msg03374.html	O-CAN-UBUNT-80716/137
Debian; Libexpat					
Debian Linux/Expat *Debian is an operating system and a distribution of Free Software. Expat is a stream-oriented XML 1.0 parser library, written in C.*					
NA	2016-06-16	4.3	Expat, when used in a parser	http://www.d	O-DEB-

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

			that has not called XML_SetHashSalt or passed it a seed of 0, makes it easier for context-dependent attackers to defeat cryptographic protection mechanisms via vectors involving use of the srand function. **Reference: CVE-2012-6702**	ebian.org/security/2016/dsa-3597	DEBIA-80716/138
Apple					
Iphone Os, safari *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware. Safari is a web browser developed by Apple based on the WebKit engine.*					
Cross Site Scripting; Gain Information	2016-06-19	5	The XSS auditor in WebKit, as used in Apple iOS before 9.3 and Safari before 9.1, does not properly handle redirects in block mode, which allows remote attackers to obtain sensitive information via a crafted URL. **Reference: CVE-2016-1864**	http://lists.apple.com/archives/security-announce/2016/Mar/msg00000.html	O-APP-IPHON-80716/139
Apple					
Airport Base Station Firmware; Iphone Os; Mac Os X; Mdnsresponder; Watchos *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware. OS X is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc.MDNSResponder, also known as Bonjour, is Apple's native zero configuration networking process for Mac that was ported over to Windows and associated with MDNSNSP.DLL. On a Mac or iOS device, this program is used for networking nearly everything. watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.*					
Denial of Service; Execute Code	2016-06-25	7.5	The handle_regservice_request function in mDNSResponder before 625.41.2 allows remote attackers to execute arbitrary code or cause a denial of service (NULL pointer dereference) via unspecified vectors. **Reference: CVE-2015-7988**	http://www.kb.cert.org/vuls/id/143335	O-APP-AIRPO-80716/140
OS					
Iodata					

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

Etx-r Firmware *ETX-R Firmware allows remote attackers to cause Denial of serviced (Web Service crash) via unspecified vectors.*					
Denial of Service	2016-06-18	5	I-O DATA DEVICE ETX-R devices allow remote attackers to cause a denial of service (web-server crash) via unspecified vectors. **Reference: CVE-2016-4821**	http://www.iodata.jp/support/information/2016/etx-r/	O-IOD-ETX-R-80716/141
Cross Site Request Forgery	2016-06-18	6.8	Cross-site request forgery (CSRF) vulnerability on I-O DATA DEVICE ETX-R devices allows remote attackers to hijack the authentication of arbitrary users. **Reference: CVE-2016-4820**	http://jvn.jp/en/jp/JVN61317238/index.html	O-IOD-ETX-R-80716/142
Buffalo					
Bhr-4grv Firmware; Dwr-hp-g300nh Firmware; Fs-600dhp Firmware; Hw-450hp-zwe Firmware; Wapm-ag300n Firmware; Wapm-apg300n Firmware; Wcr-300 Firmware; Whr-300 Firmware; Whr-300hp Firmware; Whr-hp-g300n Firmware; Wpl-05g300 Firmware; Wxr-1750dhp Firmware; Wxr-1900dhp Firmware; Wzr-1166dhp Firmware; Wzr-1166dhp2 Firmware; Wzr-1750dhp Firmware; Wzr-1750dhp2 Firmware; Wzr-300hp Firmware; Wzr-450hp Firmware; Wzr-450hp-cwt Firmware; Wzr-450hp-ub Firmware; Wzr-600dhp Firmware; Wzr-600dhp3 Firmware; Wzr-900dhp Firmware; Wzr-900dhp2 Firmware; Wzr-900dhp2 Firmware; Wzr-d1100h Firmware; Wzr-hp-ag300h Firmware; Wzr-hp-g300nh Firmware; Wzr-hp-g301nh Firmware; Wzr-hp-g302h Firmware; Wzr-hp-g450h Firmware; Wzr-s1750dhp Firmware; Wzr-s600dhp Firmware; Wzr-s900dhp Firmware *Buffalo is a global manufacturer of innovative storage, multimedia, and wireless networking products for the home and small business. The company is recognized as the Number 1 total PC peripheral manufacturer in Japan, and was the worldwide consumer NAS market leader 6 years in a row (In-Stat). The company's storage products are addressing the needs of the individual and the business, providing cost-effective network attached storage (NAS), portable and desktop hard drives, multimedia players, Wireless LAN routers and a versatile line of USB flash drives, which together offer a complete and integrated solution for the small office and digital home environment.*					
Gain Information	2016-06-18	4.3	BUFFALO WZR-600DHP3 devices with firmware 2.16 and earlier and WZR-S600DHP devices allow remote attackers to discover credentials and other sensitive information via unspecified vectors. **Reference: CVE-2016-4816**	http://jvn.jp/en/jp/JVN75813272/index.html	O-BUF-BHR-4-80716/143
Wzr-600dhp2 Firmware					

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

Buffalo’s AirStation Dual Band Gigabit router (WZR-600DHP2-EU) is one of Buffalo’s family of wireless routers.					
Directory traversal	2016-06-18	5	Directory traversal vulnerability on BUFFALO WZR-600DHP3 devices with firmware 2.16 and earlier and WZR-S600DHP devices with firmware 2.16 and earlier allows remote attackers to read arbitrary files via unspecified vectors. **Reference: CVE-2016-4815**		O-BUF-WZR-6-80716/144
Directory traversal	2016-06-18	5	Directory traversal vulnerability in kml2jsonp.php in Geospatial Information Authority of Japan (aka GSI) Old_GSI_Maps before January 2015 on Windows allows remote attackers to read arbitrary files via unspecified vectors. **Reference: CVE-2016-4814**	http://buffalo.jp/support_s/s20160527b.html	O-BUF-WZR-6-80716/145
Cisco					
IOS *Cisco IOS XE software provides a modular structure that significantly enhances software quality and performance by separating the data plane and control plan.*					
Denial of Service; Overflow	2016-06-18	6.1	Cisco IOS 15.2(1)T1.11 and 15.2(2)TST allows remote attackers to cause a denial of service (device crash) via a crafted LLDP packet, aka Bug ID CSCun63132. **Reference: CVE-2016-1424**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160616-ios	O-CIS-IOS-80716/146
Rv110w Wireless-n Vpn Firewall Firmware, Rv130w Wireless-n Multifunction Vpn Router Firmware, Rv215w Wireless-n Vpn Router Firmware *Cisco Small Business RV Series Routers offer virtual private networking (VPN) technology that lets your remote workers connect to your network through a secure Internet pathway.*					
Denial of Service ; Overflow	2016-06-18	6.8	Buffer overflow in the web-based management interface on Cisco RV110W devices with firmware before 1.2.1.7, RV130W devices with firmware before 1.0.3.16, and RV215W devices with firmware before 1.3.0.8 allows	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-	O-CIS-RV110-80716/147

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

			remote authenticated users to cause a denial of service (device reload) via crafted configuration commands in an HTTP request, aka Bug ID CSCux82523. **Reference: CVE-2016-1397**	rv2	
Cross Site Scripting	2016-06-18	4.3	Cross-site scripting (XSS) vulnerability in the web-based management interface on Cisco RV110W devices with firmware before 1.2.1.7, RV130W devices with firmware before 1.0.3.16, and RV215W devices with firmware before 1.3.0.8 allows remote attackers to inject arbitrary web script or HTML via a crafted parameter, aka Bug ID CSCux82583. **Reference: CVE-2016-1396**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-rv1	O-CIS-RV110-80716/148
Execute Code	2016-06-18	10	The web-based management interface on Cisco RV110W devices with firmware before 1.2.1.7, RV130W devices with firmware before 1.0.3.16, and RV215W devices with firmware before 1.3.0.8 allows remote attackers to execute arbitrary code as root via a crafted HTTP request, aka Bug ID CSCux82428. **Reference: CVE-2016-1395**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-rv	O-CIS-RV110-80716/149
Oslsoft					
Pi Sql Data Access Server 2016 *OSIsoft PI SQL Data Access Server (aka OLE DB) 2016 1.5 allows remote authenticated users to cause a denial of service (service outage and data loss) via a message.*					
Denial of Service	2016-06-19	4	OSIsoft PI SQL Data Access Server (aka OLE DB) 2016 1.5 allows remote authenticated users to cause a denial of service (service outage and data loss) via a message. **Reference: CVE-2016-4530**	https://techsupport.osisoft.com/Troubleshooting/Alerts/AL00300	O-OSL-PI SQ-80716/150
Apple					
Mac Os X *OS X is a series of Unix-based graphical interface operating systems (OS) developed and marketed*					

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

by Apple Inc.					
Gain Information	2016-06-19	4.3	Intel Graphics Driver in Apple OS X before 10.11.5 allows attackers to obtain sensitive kernel memory-layout information via a crafted app, a different vulnerability than CVE-2016-1860. **Reference: CVE-2016-1862**	http://lists.apple.com/archives/security-announce/2016/May/msg00004.html	O-APP-MAC O-80716/151
Denial of Service ; Execute Code Overflow; Memory Corruption	2016-06-19	9.3	The NVIDIA Graphics Drivers subsystem in Apple OS X before 10.11.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1846. **Reference: CVE-2016-1861**	http://lists.apple.com/archives/security-announce/2016/May/msg00004.html	O-APP-MAC O-80716/152
Gain Information	2016-06-19	4.3	Intel Graphics Driver in Apple OS X before 10.11.5 allows attackers to obtain sensitive kernel memory-layout information via a crafted app, a different vulnerability than CVE-2016-1862. **Reference: CVE-2016-1860**	http://lists.apple.com/archives/security-announce/2016/May/msg00004.html	O-APP-MAC O-80716/153
EMC					
Data Domain *Data Domain Corporation was an Information Technology company from 2001-2009 specializing in target-based deduplication solutions for disk based backup.*					
Bypass	2016-06-19	9	EMC Data Domain OS 5.4 through 5.7 before 5.7.2.0 allows remote authenticated users to bypass intended password-change restrictions by leveraging access to (1) a different account with the same role as a target account or (2) an account's session at an unattended workstation. **Reference: CVE-2016-0912**	http://seclists.org/bugtraq/2016/Jun/50	O-EMC-DATA-80716/154
NA	2016-06-	7.2	EMC Data Domain OS 5.4	http://seclist	O-EMC-

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

	19		through 5.7 before 5.7.2.0 has a default no_root_squash option for NFS exports, which makes it easier for remote attackers to obtain filesystem access by leveraging client root privileges. **Reference: CVE-2016-0911**	s.org/bugtraq/2016/Jun/50	DATA-80716/155
Netgear					
D3600 Firmware *NETGEAR D3600 devices with firmware 1.0.0.49 and D6000 devices with firmware 1.0.0.49 and earlier use the same hardcoded private key across different customers' installations, which allows remote attackers to defeat cryptographic protection mechanisms by leveraging knowledge of this key from another installation.*					
NA	2016-06-19	4.3	The password-recovery feature on NETGEAR D3600 devices with firmware 1.0.0.49 and D6000 devices with firmware 1.0.0.49 and earlier allows remote attackers to discover the cleartext administrator password by reading the cgi-bin/passrec.asp HTML source code. **Reference: CVE-2015-8289**	http://www.kb.cert.org/vuls/id/778696	O-NET-D3600-80716/156
NA	2016-06-19	4.3	NETGEAR D3600 devices with firmware 1.0.0.49 and D6000 devices with firmware 1.0.0.49 and earlier use the same hardcoded private key across different customers' installations, which allows remote attackers to defeat cryptographic protection mechanisms by leveraging knowledge of this key from another installation. **Reference: CVE-2015-8288**	http://www.kb.cert.org/vuls/id/778696	O-NET-D3600-80716/157
Cisco					
Asyncos *All Cisco Email Security appliances are powered by the unique Cisco AsyncOS operating system for high performance and security.*					
Bypass	2016-06-22	5	Cisco AsyncOS 9.7.0-125 on Email Security Appliance (ESA) devices allows remote attackers to bypass intended	http://tools.cisco.com/security/center/content/Ci	O-CIS-ASYNC-80716/158

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

			spam filtering via crafted executable content in a ZIP archive, aka Bug ID CSCuy39210. **Reference:CVE-2016-1438**	scoSecurityAdvisory/cisco-sa-20160622-esa	
Cisco					
Ip Phone 8800 Series Firmware *The Cisco IP Phone 8800 Series delivers HD video and VoIP communications, and integrates with your mobile device to meet your business needs.*					
NA	2016-06-22	6.2	Cisco 8800 phones with software 11.0(1) do not properly enforce mounted-filesystem permissions, which allows local users to write to arbitrary files by leveraging shell access, aka Bug ID CSCuz03014. **Reference: CVE-2016-1435**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160620-ipp	O-CIS-IPPH-80716/159
Directory Traversal	2016-06-22	4	The license-certificate upload functionality on Cisco 8800 phones with software 11.0(1) allows remote authenticated users to delete arbitrary files via an invalid file, aka Bug ID CSCuz03010. **Reference: CVE-2016-1434**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160620-ip-phone	O-CIS-IPPH-80716/160
Ios Xe *Cisco IOS XE software provides a modular structure that significantly enhances software quality and performance by separating the data plane and control plan.*					
Denial of Service	2016-06-22	6.8	Double free vulnerability in Cisco IOS XE 3.15S, 3.16S, and 3.17S allows remote authenticated users to cause a denial of service (device restart) via a sequence of crafted SNMP read requests, aka Bug ID CSCux13174. **Reference: CVE-2016-1428**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160620-iosxe	O-CIS-IOSX-80716/161
Cisco					
IOS *Cisco IOS (originally Internetwork Operating System) is a family of software used on most Cisco Systems routers and current Cisco network switches. (Earlier switches ran CatOS.) IOS is a package of routing, switching, internetworking and telecommunications functions integrated into a multitasking operating system.*					
Denial of Service	2016-06-	5	Cisco IOS 15.5(3)M on	http://tools.c	O-CIS-

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

	22		Integrated Services Router (ISR) 800, 819, and 829 devices allows remote attackers to cause a denial of service (memory consumption) via crafted TCP packets on the SSH port, aka Bug ID CSCuu13476. **Reference: CVE-2015-6289**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160620-isr	IOS-80716/162
Corega					
Cg-wlr300gnv Firmware, Cg-wlr300gnv-w Firmware *NA*					
NA	2016-06-25	5	The Wi-Fi Protected Setup (WPS) implementation on Corega CG-WLR300GNV and CG-WLR300GNV-W devices does not restrict the number of PIN authentication attempts, which makes it easier for remote attackers to obtain network access via a brute-force attack. **Reference: CVE-2016-4824**	http://corega.jp/support/security/20160622_wlr300gnv.htm	O-COR-CG-WL-80716/163
Cg-wlbaragm Firmware *Corega CG-WLBARAGM Devices Provide An Open Proxy Service, Which Allows Remote Attackers To Trigger Outbound Network Traffic Via Unspecified Vectors.*					
Denial of Service	2016-06-25	7.8	Corega CG-WLBARAGM devices allow remote attackers to cause a denial of service (reboot) via unspecified vectors. **Reference: CVE-2016-4823**	http://jvndb.jvn.jp/jvndb/JVNDB-2016-000108	O-COR-CG-WL-80716/164
Cg-wlbargnl Firmware					
Execute Code	2016-06-25	5.2	Corega CG-WLBARGL devices allow remote authenticated users to execute arbitrary commands via unspecified vectors. **Reference: CVE-2016-4822**	http://jvn.jp/en/jp/JVN76653039/index.html	O-COR-CG-WL-80716/165
Schneider-electric					
Powerlogic Pm8ecc Firmware *This firmware version addresses an issue where the device was not recovering from network vulnerability scan and addressed XSS issue with PL Tags.*					
Cross Site Scripting	2016-06-25	4.3	Cross-site scripting (XSS) vulnerability in the Schneider Electric PowerLogic PM8ECC module before 2.651 for	https://ics-cert.us-cert.gov/advisories/ICSA-	O-SCH-POWER-80716/166

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

			PowerMeter 800 devices allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-4513**	16-173-02	
Apple					
Airport Base Station Firmware; Iphone Os; Mac Os X; Mdnsresponder; Watchos *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware. OS X is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc.MDNSResponder, also known as Bonjour, is Apple's native zero configuration networking process for Mac that was ported over to Windows and associated with MDNSNSP.DLL. On a Mac or iOS device, this program is used for networking nearly everything. watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.*					
Buffer Overflow	2016-06-25	6.8	Multiple buffer overflows in mDNSResponder before 625.41.2 allow remote attackers to read or write to out-of-bounds memory locations via vectors involving the (1) GetValueForIPv4Addr, (2) GetValueForMACAddr, (3) rfc3110_import, or (4) CopyNSEC3ResourceRecord function. **Reference: CVE-2015-7987**	https://support.apple.com/HT206846	O-APP-AIRPO-80716/167
Linux					
Linux Kernel *The Linux kernel is a Unix-like computer operating system kernel.*					
Denial of Service; Overflow	2016-06-27	7.2	Multiple heap-based buffer overflows in the hiddev_ioctl_usage function in drivers/hid/usbhid/hiddev.c in the Linux kernel through 4.6.3 allow local users to cause a denial of service or possibly have unspecified other impact via a crafted (1) HIDIOCGUSAGES or (2) HIDIOCSUSAGES ioctl call. **Reference: CVE-2016-5829**	http://www.openwall.com/lists/oss-security/2016/06/26/2	O-LIN-LINUX-80716/168
Denial of Service	2016-06-27	7.2	The start_thread function in arch/powerpc/kernel/process.c in the Linux kernel through 4.6.3 on powerpc platforms mishandles transactional	http://www.openwall.com/lists/oss-security/2016/06/25/7	O-LIN-LINUX-80716/169

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

			state, which allows local users to cause a denial of service (invalid process state or TM Bad Thing exception, and system crash) or possibly have unspecified other impact by starting and suspending a transaction before an exec system call. **Reference: CVE-2016-5828**		
Denial of Service; Overflow ; Memory Corruption; Gain Information	2016-06-27	5.6	Race condition in the vop_ioctl function in drivers/misc/mic/vop/vop_vringh.c in the MIC VOP driver in the Linux kernel before 4.6.1 allows local users to obtain sensitive information from kernel memory or cause a denial of service (memory corruption and system crash) by changing a certain header, aka a "double fetch" vulnerability. **Reference: CVE-2016-5728**	https://github.com/torvalds/linux/commit/9bf292bfca94694a721449e3fd752493856710f6	O-LIN-LINUX-80716/170
Gain Information	2016-06-27	5	The rds_inc_info_copy function in net/rds/recv.c in the Linux kernel through 4.6.3 does not initialize a certain structure member, which allows remote attackers to obtain sensitive information from kernel stack memory by reading an RDS message. **Reference: CVE-2016-5244**	http://www.openwall.com/lists/oss-security/2016/06/03/5	O-LIN-LINUX-80716/171
Gain Information	2016-06-27	2.1	The tipc_nl_compat_link_dump function in net/tipc/netlink_compat.c in the Linux kernel through 4.6.3 does not properly copy a certain string, which allows local users to obtain sensitive information from kernel stack memory by reading a Netlink message. **Reference: CVE-2016-5243**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=5d2be1422e02ccd697ccfcd45c85b4a26e6178e2	O-LIN-LINUX-80716/172
Denial of Service	2016-06-27	4.9	The key_reject_and_link function in security/keys/key.c in the Linux kernel through	http://git.kernel.org/cgit/linux/kernel/	O-LIN-LINUX-80716/17

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

			4.6.3 does not ensure that a certain data structure is initialized, which allows local users to cause a denial of service (system crash) via vectors involving a crafted keyctl request2 command. **Reference: CVE-2016-4470**	git/torvalds/linux.git/commit/?id=38327424b40bcebe2de92d07312c89360ac9229a	3
Denial of Service; Execute Code	2016-06-27	7.2	arch/x86/kvm/vmx.c in the Linux kernel through 4.6.3 mishandles the APICv on/off state, which allows guest OS users to obtain direct APIC MSR access on the host OS, and consequently cause a denial of service (host OS crash) or possibly execute arbitrary code on the host OS, via x2APIC mode. **Reference: CVE-2016-4440**	http://www.openwall.com/lists/oss-security/2016/05/20/2	O-LIN-LINUX-80716/174
Siemens					
Simatic S7-300 With Profitnet Support Firmware; Simatic S7-300 Without Profitnet Support Firmware *The SIMATIC S7-300 universal Controllers saves on installation space and features a modular design. A wide range of modules can be used to expand the system centrally or to create decentralized structures according to the task at hand, and facilitates a cost-effective stock of spare parts. SIMATIC is known for continuity and quality.*					
Denial of Service	2016-06-27	7.8	Siemens SIMATIC S7-300 Profinet-enabled CPU devices with firmware before 3.2.12 and SIMATIC S7-300 Profinet-disabled CPU devices with firmware before 3.3.12 allow remote attackers to cause a denial of service (defect-mode transition) via crafted (1) ISO-TSAP or (2) Profibus packets. **Reference: CVE-2016-3949**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-818183.pdf	O-SIE-SIMAT-80716/175
Linux					
Linux Kernel *The Linux kernel is a Unix-like computer operating system kernel.*					
Denial of Service; Gain Information	2016-06-27	5.6	The msr_mtrr_valid function in arch/x86/kvm/mtrr.c in the Linux kernel before 4.6.1 supports MSR 0x2f8, which allows guest OS users to read or write to the kvm_arch_vcpu	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?	O-LIN-LINUX-80716/176

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

			data structure, and consequently obtain sensitive information or cause a denial of service (system crash), via a crafted ioctl call. **Reference: CVE-2016-3713**	id=9842df62004f366b9fed2423e24df10542ee0dc5	
Linux Kernel-rt *RTLinux is a hard realtime RTOS microkernel that runs the entire Linux operating system as a fully preemptive process.*					
Execute Code	2016-06-27	6.8	The icmp_check_sysrq function in net/ipv4/icmp.c in the kernel.org projects/rt patches for the Linux kernel, as used in the kernel-rt package before 3.10.0-327.22.1 in Red Hat Enterprise Linux for Real Time 7 and other products, allows remote attackers to execute SysRq commands via crafted ICMP Echo Request packets, as demonstrated by a brute-force attack to discover a cookie, or an attack that occurs after reading the local icmp_echo_sysrq file. **Reference: CVE-2016-3707**	http://www.openwall.com/lists/oss-security/2016/05/17/1	O-LIN-LINUX-80716/177
Linux Kernel *The Linux kernel is a Unix-like computer operating system kernel.*					
Denial of Service; Overflow; Gain Privileges	2016-06-27	7.2	The ecryptfs_privileged_open function in fs/ecryptfs/kthread.c in the Linux kernel before 4.6.3 allows local users to gain privileges or cause a denial of service (stack memory consumption) via vectors involving crafted mmap calls for /proc pathnames, leading to recursive pagefault handling. **Reference: CVE-2016-1583**	https://github.com/torvalds/linux/commit/2f36db71009304b3f0b95afacd8eba1f9f046b87	O-LIN-LINUX-80716/178
Overflow; Gain Privileges	2016-06-27	7.2	Integer overflow in lib/asn1_decoder.c in the Linux kernel before 4.6 allows local users to gain privileges via crafted ASN.1 data. **Reference: CVE-2016-0758**	http://www.openwall.com/lists/oss-security/2016/05/12/9	O-LIN-LINUX-80716/179

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

Linux					
Linux Kernel *The Linux kernel is a Unix-like computer operating system kernel.*					
Denial of Service; Overflow	2016-06-27	7.2	The snd_compress_check_input function in sound/core/compress_offload.c in the ALSA subsystem in the Linux kernel before 3.17 does not properly check for an integer overflow, which allows local users to cause a denial of service (insufficient memory allocation) or possibly have unspecified other impact via a crafted SNDRV_COMPRESS_SET_PARAMS ioctl call. **Reference: CVE-2014-9904**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6217e5ede23285ddfee10d2e4ba0cc2d4c046205	O-LIN-LINUX-80716/180
Gain Information	2016-06-27	2.1	The sched_read_attr function in kernel/sched/core.c in the Linux kernel 3.14-rc before 3.14-rc4 uses an incorrect size, which allows local users to obtain sensitive information from kernel stack memory via a crafted sched_getattr system call. **Reference: CVE-2014-9903**	https://github.com/torvalds/linux/commit/4efbc454ba68def5ef285b26ebfcfdb605b52755	O-LIN-LINUX-80716/181
Linux					
Linux Kernel *The Linux kernel is a Unix-like computer operating system kernel.*					
Bypass	2016-06-29	4.9	nfsd in the Linux kernel through 4.6.3 allows local users to bypass intended file-permission restrictions by setting a POSIX ACL, related to nfs2acl.c, nfs3acl.c, and nfs4acl.c. **Reference: CVE-2016-1237**	https://github.com/torvalds/linux/commit/999653786df6954a31044528ac3f7a5dadca08f4	O-LIN-LINUX-80716/182
Denial of Service; Overflow	2016-06-29	7.2	Integer overflow in the snd_compr_allocate_buffer function in sound/core/compress_offload.c in the ALSA subsystem in the Linux kernel before 3.6-rc6-next-20120917 allows	https://github.com/torvalds/linux/commit/b35cc8225845112a616e3a2266d2fde5ab1	O-LIN-LINUX-80716/183

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

			local users to cause a denial of service (insufficient memory allocation) or possibly have unspecified other impact via a crafted SNDRV_COMPRESS_SET_PARAMS ioctl call. **Reference: CVE-2012-6703**	3d3ab	
Hardware/ Application(H/A)					
Moxa					
Pt-7728, Pt-7728 Firmware *The PowerTrans PT-7728 is designed to meet the demands of power substation automation systems (IEC 61850-3, IEEE 1613), traffic control systems (NEMA TS2), and railway applications (EN50121-4). The PT-7728's Gigabit and fast Ethernet backbone, redundant ring, and 24/48 VDC or 110/220 VDC/VAC dual isolated redundant power supplies increase the reliability of your communications and save on cabling/wiring costs.*					
NA	2016-06-19	4.6	Moxa PT-7728 devices with software 3.4 build 15081113 allow remote authenticated users to change the configuration via vectors involving a local proxy. **Reference: CVE-2016-4514**	https://ics-cert.us-cert.gov/advisories/ICSA-16-168-01	H-MOX-PT-77-80716/184
Hardware(H)					
Huawei					
Huawei Firmware					
Denial of Service	2016-06-24	7.1	Memory leak in Huawei IPS Module, NGFW Module, NIP6300, NIP6600, and Secospace USG6300, USG6500, USG6600, USG9500, and AntiDDoS8000 V500R001C00 before V500R001C20SPC100, when in hot standby networking where two devices are not directly connected, allows remote attackers to cause a denial of service (memory consumption and reboot) via a crafted packet. **Reference: CVE-2016-5435**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160615-01-standby-en	H-HUA-HUAWE-80716/185

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

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