National Critical Information Infrastructure Protection Centre

CVE Report

01-15 July 2016

Vol. 3 No.12

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Application (A)					
Accela					
Civic Platform Citizen Access Portal *Accela Civic Platform Citizen Access portal relies on the client to restrict file types for uploads, which allows remote authenticated users to execute arbitrary code via modified _EventArgument and filename parameters.*					
Execute Code	2016-07-12	6.8	applications/core/modules/front/system/content.php in Invision Power Services IPS Community Suite (aka Invision Power Board, IPB, or Power Board) before 4.1.13, when used with PHP before 5.4.24 or 5.5.x before 5.5.8, allows remote attackers to execute arbitrary code via the content_class parameter. **Reference: CVE-2016-6174**	http://seclists.org/fulldisclosure/2016/Jul/19	A-ACC-CIVIC-250716/01
Denial of Service	2016-07-06	4	ISC BIND through 9.9.9-P1, 9.10.x through 9.10.4-P1, and 9.11.x through 9.11.0b1 allows primary DNS servers to cause a denial of service (secondary DNS server crash) via a large AXFR response, and possibly allows IXFR servers to cause a denial of service (IXFR client crash) via a large IXFR response and allows remote authenticated users to cause a denial of service (primary DNS server crash) via a large UPDATE message. **Reference: CVE-2016-6170**	https://lists.dns-oarc.net/pipermail/dns-operations/2016-July/015075.html	A-ACC-CIVIC-250716/02
Adobe					
Acrobat; Acrobat Dc; Acrobat Reader Dc; Reader *Use Acrobat to convert, edit and sign PDF files at your desk or on the go. Adobe Acrobat DC is a trusted PDF creator. Adobe Acrobat Reader DC software is the free global standard for reliably viewing, printing, and commenting on PDF documents. Adobe Reader is the most popular program in the world for viewing, creating, managing and*					

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

manipulating PDF (Portable Document Format) files.					
Gain Information	2016-07-03	1.9	Race condition in the sclp_ctl_ioctl_sccb function in drivers/s390/char/sclp_ctl.c in the Linux kernel before 4.6 allows local users to obtain sensitive information from kernel memory by changing a certain length value, aka a "double fetch" vulnerability. **Reference: CVE-2016-6130**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=532c34b5fbf1687df63b3fcd5b2846312ac943c6	A-ADO-ACROB-250716/03
Cross Site Scripting	2016-07-12	3.5	Cross-site scripting (XSS) vulnerability in the volume backup service module in Huawei Public Cloud Solution before 1.0.5 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-5850**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160629-01-publiccloud-en	A-ADO-ACROB-250716/04
Gain Information	2016-07-04	1.9	Siemens SICAM PAS through 8.07 allows local users to obtain sensitive configuration information by leveraging database stoppage. **Reference: CVE-2016-5849**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-444217.pdf	A-ADO-ACROB-250716/05
NA	2016-07-04	1.7	Siemens SICAM PAS before 8.07 does not properly restrict password data in the database, which makes it easier for local users to calculate passwords by leveraging unspecified database privileges. **Reference: CVE-2016-5848**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-444217.pdf	A-ADO-ACROB-250716/06
Gain Privileges	2016-07-13	7.2	Huawei HiSuite before 4.0.4.204_ove (Out of China) and before 4.0.4.301 (China) use a weak ACL (FILE_WRITE_DATA for BUILTIN\Users) for the HiSuite service directory, which allows local users to gain SYSTEM privileges via a Trojan horse (1) SspiCli.dll or (2) USERENV.dll file or	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160624-01-hisuite-en	A-ADO-ACROB-250716/07

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

			possibly other unspecified DLL files. **Reference: CVE-2016-5821**		
Execute Code; Overflow	2016-07-11	6.8	Stack-based buffer overflow in WECON LeviStudio allows remote attackers to execute arbitrary code via a crafted file. **Reference: CVE-2016-5781**	https://ics-cert.us-cert.gov/advisories/ICSA-16-189-01	A-ADO-ACROB-250716/08
Gain Information	2016-07-12	4.3	The HTTPS server in Blue Coat PacketShaper S-Series 11.5.x before 11.5.3.2 might allow remote attackers to obtain sensitive credentials and other information via unspecified vectors, related to use of insecure cryptographic parameters. **Reference: CVE-2016-5774**	https://bto.bluecoat.com/security-advisory/sa127	A-ADO-ACROB-250716/09
Gain Information; Cross Site Request Forgery	2016-07-02	5	The Transformation implementation in phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 does not use the no-referrer Content Security Policy (CSP) protection mechanism, which makes it easier for remote attackers to conduct CSRF attacks by reading an authentication token in a Referer header, related to libraries/Header.php. **Reference: CVE-2016-5739**	https://github.com/phpmyadmin/phpmyadmin/commit/1e5716cb96d46efc305381ae0da08e73fe340f05	A-ADO-ACROB-250716/10
Execute Code	2016-07-02	7.5	phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 does not properly choose delimiters to prevent use of the preg_replace e (aka eval) modifier, which might allow remote attackers to execute arbitrary PHP code via a crafted string, as demonstrated by the table search-and-replace implementation. **Reference: CVE-2016-5734**	https://www.phpmyadmin.net/security/PMASA-2016-27/	A-ADO-ACROB-250716/11

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

Cross Site Scripting	2016-07-02	4.3	Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) a crafted table name that is mishandled during privilege checking in table_row.phtml, (2) a crafted mysqld log_bin directive that is mishandled in log_selector.phtml, (3) the Transformation implementation, (4) AJAX error handling in js/ajax.js, (5) the Designer implementation, (6) the charts implementation in js/tbl_chart.js, or (7) the zoom-search implementation in rows_zoom.phtml. **Reference: CVE-2016-5733**	https://www.phpmyadmin.net/security/PMASA-2016-26/	A-ADO-ACROB-250716/12
Cross Site Scripting	2016-07-02	4.3	Multiple cross-site scripting (XSS) vulnerabilities in the partition-range implementation in templates/table/structure/display_partitions.phtml in the table-structure page in phpMyAdmin 4.6.x before 4.6.3 allow remote attackers to inject arbitrary web script or HTML via crafted table parameters. **Reference: CVE-2016-5732**	https://www.phpmyadmin.net/security/PMASA-2016-25/	A-ADO-ACROB-250716/13
Cross Site Scripting	2016-07-02	4.3	Cross-site scripting (XSS) vulnerability in examples/openid.php in phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 allows remote attackers to inject arbitrary web script or HTML via vectors involving an OpenID error message. **Reference: CVE-2016-5731**	https://github.com/phpmyadmin/phpmyadmin/commit/418aeea3d83b0b6021bac311d849570acfc6e48c	A-ADO-ACROB-250716/14

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

Gain Information	2016-07-02	5	phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 allows remote attackers to obtain sensitive information via vectors involving (1) an array value to FormDisplay.php, (2) incorrect data to validate.php, (3) unexpected data to Validator.php, (4) a missing config directory during setup, or (5) an incorrect OpenID identifier data type, which reveals the full path in an error message. **Reference: CVE-2016-5730**	https://www.phpmyadmin.net/security/PMASA-2016-23/	A-ADO-ACROB-250716/15
Denial of Service	2016-07-02	5	js/get_scripts.js.php in phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 allows remote attackers to cause a denial of service via a large array in the scripts parameter. **Reference: CVE-2016-5706**	https://www.phpmyadmin.net/security/PMASA-2016-22/	A-ADO-ACROB-250716/16
Cross Site Scripting	2016-07-02	4.3	Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.4.x before 4.4.15.7 and 4.6.x before 4.6.3 allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) server-privileges certificate data fields on the user privileges page, (2) an "invalid JSON" error message in the error console, (3) a database name in the central columns implementation, (4) a group name, or (5) a search name in the bookmarks implementation. **Reference: CVE-2016-5705**	https://www.phpmyadmin.net/security/PMASA-2016-21/	A-ADO-ACROB-250716/17
Cross Site Scripting	2016-07-02	4.3	Cross-site scripting (XSS) vulnerability in the table-structure page in phpMyAdmin 4.6.x before 4.6.3 allows remote	https://www.phpmyadmin.net/security/PMASA-2016-20/	A-ADO-ACROB-250716/18

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

			attackers to inject arbitrary web script or HTML via vectors involving a comment. **Reference: CVE-2016-5704**		
Execute Code; SQL Injection	2016-07-02	7.5	SQL injection vulnerability in libraries/central_columns.lib.php in phpMyAdmin 4.4.x before 4.4.15.7 and 4.6.x before 4.6.3 allows remote attackers to execute arbitrary SQL commands via a crafted database name that is mishandled in a central column query. **Reference: CVE-2016-5703**	https://www.phpmyadmin.net/security/PMASA-2016-19/	A-ADO-ACROB-250716/19
NA	2016-07-02	4.3	phpMyAdmin 4.6.x before 4.6.3, when the environment lacks a PHP_SELF value, allows remote attackers to conduct cookie-attribute injection attacks via a crafted URI. **Reference: CVE-2016-5702**	https://www.phpmyadmin.net/security/PMASA-2016-18/	A-ADO-ACROB-250716/20
NA	2016-07-02	4.3	setup/frames/index.inc.php in phpMyAdmin 4.0.10.x before 4.0.10.16, 4.4.15.x before 4.4.15.7, and 4.6.x before 4.6.3 allows remote attackers to conduct BBCode injection attacks against HTTP sessions via a crafted URI. **Reference: CVE-2016-5701**	https://github.com/phpmyadmin/phpmyadmin/commit/1dca386505f396f0c2035112a403cc80768a141f	A-ADO-ACROB-250716/21
Denial of Service; Overflow Memory Corruption	2016-07-11	7.1	The Client Intrusion Detection System (CIDS) driver before 15.0.6 in Symantec Endpoint Protection (SEP) and before 15.1.2 in Norton Security allows remote attackers to cause a denial of service (memory corruption and system crash) via a malformed Portable Executable (PE) file. **Reference: CVE-2016-5308**	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160707_01	A-ADO-ACROB-250716/22
Execute Code; Overflow	2016-07-02	10	Stack-based buffer overflow in the PlayMacro function in	http://community.microfocus.co	A-ADO-ACROB-250716/23

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

			ObjectXMacro.ObjectXMacro in WdMacCtl.ocx in Micro Focus Rumba 9.x before 9.3 HF 11997 and 9.4.x before 9.4 HF 12815 allows remote attackers to execute arbitrary code via a long MacroName argument. NOTE: some references mention CVE-2016-5226 but that is not a correct ID for any Rumba vulnerability. **Reference: CVE-2016-5228**	m/microfocus/mainframe_solutions/rumba/w/knowledge_base/28600.micro-focus-rumba-9-x-security-update.aspx	
Bypass	2016-07-13	2.1	Citrix Worx Home for iOS before 10.3.6 and XenMobile MDX Toolkit for iOS before 10.3.6 might allow physically proximate attackers to bypass in-application Apple Touch ID authentication via unspecified vectors, related to an application requiring re-authentication. **Reference: CVE-2016-5109**	http://support.citrix.com/article/CTX214006	A-ADO-ACROB-250716/24
Flash Player *Adobe Flash Player (labeled Shockwave Flash in Internet Explorer and Firefox) is freeware software for using content created on the Adobe Flash platform, including viewing multimedia, executing rich Internet applications, and streaming video and audio.*					
Cross Site Scripting	2016-07-04	4.3	Cross-site scripting (XSS) vulnerability in phpMyAdmin 4.4.x before 4.4.15.6 and 4.6.x before 4.6.2 allows remote attackers to inject arbitrary web script or HTML via special characters that are mishandled during double URL decoding. **Reference: CVE-2016-5099**	https://github.com/phpmyadmin/phpmyadmin/commit/b061096abd992801fbbd805ef6ff74e627528780	A-ADO-FLASH-250716/25
Directory Traversal	2016-07-04	5	Directory traversal vulnerability in libraries/error_report.lib.php in phpMyAdmin before 4.6.2-prerelease allows remote attackers to determine the existence of arbitrary files by triggering an error. **Reference: CVE-2016-5098**	https://github.com/phpmyadmin/phpmyadmin/commit/d2dc9481d2af25b035778c67eaf0bfd2d2c59dd8	A-ADO-FLASH-250716/26

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

Gain Information	2016-07-04	5	phpMyAdmin before 4.6.2 places tokens in query strings and does not arrange for them to be stripped before external navigation, which allows remote attackers to obtain sensitive information by reading (1) HTTP requests or (2) server logs. **Reference: CVE-2016-5097**	https://github.com/phpmyadmin/phpmyadmin/commit/8326aaebe54083d9726e153abdd303a141fe5ad3	A-ADO-FLASH-250716/27
Directory Traversal	2016-07-13	4	Directory traversal vulnerability in Fortinet FortiWeb before 5.5.3 allows remote authenticated administrators with read and write privileges to read arbitrary files by leveraging the autolearn feature. **Reference: CVE-2016-5092**	http://fortiguard.com/advisory/fortiweb-path-traversal-vulnerability	A-ADO-FLASH-250716/28
Denial of Service	2016-07-12	4	The handle_command function in mon/Monitor.cc in Ceph allows remote authenticated users to cause a denial of service (segmentation fault and ceph monitor crash) via an (1) empty or (2) crafted prefix. **Reference: CVE-2016-5009**	https://github.com/ceph/ceph/pull/9700	A-ADO-FLASH-250716/29
Bypass	2016-07-13	4.3	libvirt before 2.0.0 improperly disables password checking when the password on a VNC server is set to an empty string, which allows remote attackers to bypass authentication and establish a VNC session by connecting to the server. **Reference: CVE-2016-5008**	http://security.libvirt.org/2016/0001.html	A-ADO-FLASH-250716/30
Denial of Service; Overflow; Gain Information	2016-07-03	5.6	The IPT_SO_SET_REPLACE setsockopt implementation in the netfilter subsystem in the Linux kernel before 4.6 allows local users to cause a denial of service (out-of-bounds read) or possibly obtain sensitive information from kernel heap memory by leveraging in-container root access to provide a	https://github.com/torvalds/linux/commit/6e94e0cfb0887e4013b3b930fa6ab1fe6bb6ba91	A-ADO-FLASH-250716/31

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

			crafted offset value that leads to crossing a ruleset blob boundary. **Reference: CVE-2016-4998**		
Denial of Service; Gain Privileges; Memory Corruption	2016-07-03	7.2	The compat IPT_SO_SET_REPLACE setsockopt implementation in the netfilter subsystem in the Linux kernel before 4.6.3 allows local users to gain privileges or cause a denial of service (memory corruption) by leveraging in-container root access to provide a crafted offset value that triggers an unintended decrement. **Reference: CVE-2016-4997**	https://github.com/torvalds/linux/commit/ce683e5f9d045e5d67d1312a42b359cb2ab2a13c	A-ADO-FLASH-250716/32
Denial of Service; Execute Code	2016-07-12	6.8	Use-after-free vulnerability in the xcf_load_image function in app/xcf/xcf-load.c in GIMP allows remote attackers to cause a denial of service (program crash) or possibly execute arbitrary code via a crafted XCF file. **Reference: CVE-2016-4994**	https://bugzilla.gnome.org/show_bug.cgi?id=767873	A-ADO-FLASH-250716/33
Gain Information	2016-07-12	5	The ironic-api service in OpenStack Ironic before 4.2.5 (Liberty) and 5.x before 5.1.2 (Mitaka) allows remote attackers to obtain sensitive information about a registered node by leveraging knowledge of the MAC address of a network card belonging to that node and sending a crafted POST request to the v1/drivers/$DRIVER_NAME/vendor_passthru resource. **Reference: CVE-2016-4985**	https://bugs.launchpad.net/ironic/+bug/1572796	A-ADO-FLASH-250716/34
Bypass	2016-07-06	5	The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the "SSLVerifyClient require" directive for HTTP/2 request authorization, which allows remote attackers to	http://www.apache.org/dist/httpd/CHANGES_2.4	A-ADO-FLASH-250716/35

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

			bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation. **Reference: CVE-2016-4979**		
Exec Code	2016-07-13	7.5	Apache Qpid AMQP 0-x JMS client before 6.0.4 and JMS (AMQP 1.0) before 0.10.0 does not restrict the use of classes available on the classpath, which might allow remote attackers to deserialize arbitrary objects and execute arbitrary code by leveraging a crafted serialized object in a JMS ObjectMessage that is handled by the getObject function. **Reference: CVE-2016-4974**	https://issues.apache.org/jira/browse/QPIDJMS-188	A-ADO-FLASH-250716/36
Denial of Service	2016-07-04	5	ntpd in NTP before 4.2.8p8 allows remote attackers to cause a denial of service (daemon crash) via a crypto-NAK packet. NOTE: this vulnerability exists because of an incorrect fix for CVE-2016-1547. **Reference: CVE-2016-4957**	http://support.ntp.org/bin/view/Main/SecurityNotice	A-ADO-FLASH-250716/37
Denial of Service	2016-07-04	5	ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (interleaved-mode transition and time change) via a spoofed broadcast packet. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-1548. **Reference: CVE-2016-4956**	http://support.ntp.org/bin/view/Main/SecurityNotice	A-ADO-FLASH-250716/38
Denial of Service	2016-07-04	2.6	ntpd in NTP 4.x before 4.2.8p8, when autokey is enabled, allows remote attackers to cause a denial of service (peer-variable clearing and association outage) by sending (1) a spoofed crypto-NAK packet or (2) a packet with an	http://support.ntp.org/bin/view/Main/SecurityNotice	A-ADO-FLASH-250716/39

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

			incorrect MAC value at a certain time. **Reference: CVE-2016-4955**		
Denial of Service	2016-07-04	4.3	The process_packet function in ntp_proto.c in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (peer-variable modification) by sending spoofed packets from many source IP addresses in a certain scenario, as demonstrated by triggering an incorrect leap indication. **Reference: CVE-2016-4954**	http://support.ntp.org/bin/view/Main/SecurityNotice	A-ADO-FLASH-250716/40
Denial of Service	2016-07-04	4.3	ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (ephemeral-association demobilization) by sending a spoofed crypto-NAK packet with incorrect authentication data at a certain time. **Reference: CVE-2016-4953**	http://support.ntp.org/bin/view/Main/SecurityNotice	A-ADO-FLASH-250716/41
Gain Privileges	2016-07-11	7.2	Untrusted search path vulnerability in LINE and LINE Installer 4.7.0 and earlier on Windows allows local users to gain privileges via a Trojan horse DLL in an unspecified directory. **Reference: CVE-2016-4831**	http://linecorp.com/ja/security/article/61	A-ADO-FLASH-250716/42
Gain Privileges	2016-07-02	3.7	Untrusted search path vulnerability in Flexera InstallAnywhere allows local users to gain privileges via a Trojan horse DLL in the current working directory of a setup-launcher executable file. **Reference: CVE-2016-4560**	https://flexeracommunity.force.com/customer/articles/INFO/Best-Practices-to-Avoid-Windows-Setup-Launcher-Executable-Issues	A-ADO-FLASH-250716/43
Execute Code; Overflow	2016-07-11	6.8	Heap-based buffer overflow in WECON LeviStudio allows remote attackers to execute arbitrary code via a crafted file. **Reference: CVE-2016-4533**	https://ics-cert.us-cert.gov/advisories/ICSA-16-189-01	A-ADO-FLASH-250716/44
Execute Code;	2016-07-03	7.5	Stack-based buffer overflow	https://ics-	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**

Overflow			in ELCSimulator in Eaton ELCSoft 2.4.01 and earlier allows remote attackers to execute arbitrary code via a long packet. **Reference: CVE-2016-4512**	cert.us-cert.gov/advisories/ICSA-16-182-01	250716/45
Execute Code; Overflow	2016-07-03	6	Heap-based buffer overflow in elcsoft.exe in Eaton ELCSoft 2.4.01 and earlier allows remote authenticated users to execute arbitrary code via a crafted file. **Reference: CVE-2016-4509**	https://ics-cert.us-cert.gov/advisories/ICSA-16-182-01	A-ADO-FLASH-250716/46
Cross Site Scripting	2016-07-06	4.3	Cross-site scripting (XSS) vulnerability in Rexroth Bosch BLADEcontrol-WebVIS 3.0.2 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-4508**	https://ics-cert.us-cert.gov/advisories/ICSA-16-187-01	A-ADO-FLASH-250716/47
Execute Code; SQL Injection	2016-07-06	5.5	SQL injection vulnerability in Rexroth Bosch BLADEcontrol-WebVIS 3.0.2 and earlier allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors. **Reference: CVE-2016-4507**	https://ics-cert.us-cert.gov/advisories/ICSA-16-187-01	A-ADO-FLASH-250716/48
Bypass	2016-07-11	5	Moxa Device Server Web Console 5232-N allows remote attackers to bypass authentication, and consequently modify settings and data, via vectors related to reading a cookie parameter containing a UserId value. **Reference: CVE-2016-4503**	https://ics-cert.us-cert.gov/advisories/ICSA-16-189-02	A-ADO-FLASH-250716/49
Denial of Service	2016-07-04	5	The URLValidator class in Apache Struts 2 2.3.20 through 2.3.28.1 and 2.5.x before 2.5.1 allows remote attackers to cause a denial of service via a null value for a URL field. **Reference: CVE-2016-4465**	https://bugzilla.redhat.com/show_bug.cgi?id=1348253	A-ADO-FLASH-250716/50
Denial of Service;	2016-07-08	5	Stack-based buffer overflow	https://issues.a	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**

Overflow			in Apache Xerces-C++ before 3.1.4 allows context-dependent attackers to cause a denial of service via a deeply nested DTD. **Reference: CVE-2016-4463**	pache.org/jira/secure/ReleaseNote.jspa?projectId=10510&version=12336069	250716/51
Execute Code	2016-07-04	7.5	The REST plugin in Apache Struts 2 2.3.20 through 2.3.28.1 allows remote attackers to execute arbitrary code via a crafted expression. **Reference: CVE-2016-4438**	https://bugzilla.redhat.com/show_bug.cgi?id=1348238	A-ADO-FLASH-250716/52
Bypass	2016-07-04	5	Apache Struts 2 2.3.20 through 2.3.28.1 allows remote attackers to bypass intended access restrictions and conduct redirection attacks via a crafted request. **Reference: CVE-2016-4433**	https://bugzilla.redhat.com/show_bug.cgi?id=1348251	A-ADO-FLASH-250716/53
Bypass	2016-07-04	5	Apache Struts 2 2.3.20 through 2.3.28.1 allows remote attackers to bypass intended access restrictions and conduct redirection attacks by leveraging a default method. **Reference: CVE-2016-4431**	https://bugzilla.redhat.com/show_bug.cgi?id=1348252	A-ADO-FLASH-250716/54
Cross Site Request Forgery	2016-07-04	6.8	Apache Struts 2 2.3.20 through 2.3.28.1 mishandles token validation, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks via unspecified vectors. **Reference: CVE-2016-4430**	https://bugzilla.redhat.com/show_bug.cgi?id=1348249	A-ADO-FLASH-250716/55
Cross Site Scripting	2016-07-12	3.5	Cross-site scripting (XSS) vulnerability in OpenStack Dashboard (Horizon) 8.0.1 and earlier and 9.0.0 through 9.0.1 allows remote authenticated users to inject arbitrary web script or HTML by injecting an AngularJS template in a dashboard form. **Reference: CVE-2016-4428**	https://bugs.launchpad.net/horizon/+bug/1567673	A-ADO-FLASH-250716/56
Execute Code	2016-07-08	6.8	Use-after-free vulnerability in LibreOffice before 5.1.4 allows remote attackers to	http://www.libreoffice.org/about-	A-ADO-FLASH-250716/57

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

			execute arbitrary code via a crafted RTF file, related to stylesheet and superscript tokens. **Reference: CVE-2016-4324**	us/security/advisories/cve-2016-4324/	
Execute Code	2016-07-12	6.8	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference: CVE-2016-4255**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-ADO-FLASH-250716/58
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, and CVE-2016-4252. **Reference: CVE-2016-4254**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-ADO-FLASH-250716/59
Denial of Service; Execute Code; Overflow;	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic	https://helpx.adobe.com/security/products/acro	A-ADO-FLASH-250716/60

Memory Corruption			before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, and CVE-2016-4254. **Reference: CVE-2016-4252**	bat/apsb16-26.html	
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-ADO-FLASH-250716/61

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

			2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4251**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4250**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-ADO-FLASH-250716/62
Execute Code; Overflow	2016-07-12	10	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors. **Reference: CVE-2016-4249**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-ADO-FLASH-250716/63
Execute Code	2016-07-12	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and	https://helpx.adobe.com/security/products/flash-player/apsb16-	A-ADO-FLASH-250716/64

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

			before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, and CVE-2016-4231. **Reference: CVE-2016-4248**	25.html	
Gain Information	2016-07-12	4.3	Race condition in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-4247**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-ADO-FLASH-250716/65
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243,	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-ADO-FLASH-250716/66

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

			CVE-2016-4244, and CVE-2016-4245. **Reference: CVE-2016-4246**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, and CVE-2016-4246. **Reference: CVE-2016-4245**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-ADO-FLASH-250716/67
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-ADO-FLASH-250716/68

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

			2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4244**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4243**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-ADO-FLASH-250716/69
Denial of Service; Execute Code; Overflow;	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on	https://helpx.adobe.com/security/products/flas	A-ADO-FLASH-250716/70

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

Memory Corruption			Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4242**	h-player/apsb16-25.html	
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-ADO-FLASH-250716/71

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

			2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4241**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4240**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-ADO-FLASH-250716/72
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-ADO-FLASH-250716/73

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

			unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4239**		
Xmp Toolkit *The XMP Toolkit SDK allows you to integrate XMP functionality into your product or solution.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4239,	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-ADO-XMPT-250716/74

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

			CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4238**		
Apache					
Amqp 0-x Jms Client; Jms Client Amqp *Qpid JMS client for AMQP 0-10 is a clientwhich supports the older version of the AMQP protocol 0-10.The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for message-oriented middleware*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4237**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-APA-AMQP - 250716/75
Http Server *The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on	https://helpx.adobe.com/security/products/flash-player/apsb16-	A-APA-HTTP - 250716/76

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

			Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4236**	25.html	
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-APA-HTTP - 250716/77

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

			4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4235**		
Struts *Apache Struts is a discontinued open-source web application framework for developing Java EE web applications.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4234**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-APA-STRUT-250716/78
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-APA-STRUT-250716/79

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

			unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4233**		
Gain Information	2016-07-12	5	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to obtain sensitive information from process memory via unspecified vectors. **Reference: CVE-2016-4232**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-APA-STRUT-250716/80
Execute Code	2016-07-12	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, and CVE-2016-4248. **Reference: CVE-2016-4231**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-APA-STRUT-250716/81

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

Execute Code	2016-07-12	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4231, and CVE-2016-4248. **Reference: CVE-2016-4230**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-APA-STRUT-250716/82
Execute Code	2016-07-12	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248. **Reference: CVE-2016-4229**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-APA-STRUT-250716/83
Execute Code	2016-07-12	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248. **Reference: CVE-2016-4228**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-APA-STRUT-250716/84

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

Execute Code	2016-07-12	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248. **Reference: CVE-2016-4227**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-APA-STRUT-250716/85
Blue Coat					
Packetshaper S-series *The PacketShaper S-Series products are designed to meet the needs of today's demanding enterprise network environments*					
Execute Code	2016-07-12	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248. **Reference: CVE-2016-4226**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-BLU-PACKE-250716/86
Canonical, Redhat					
Openstack Ironic; Openstack *Ironic is an OpenStack project which provisions physical hardware as opposed to virtual machines.OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter, all managed through a dashboard that gives administrators control while empowering their users to provision resources through a web interface.*					
Execute Code	2016-07-12	6.8	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-CAN-OPENS-250716/87

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

			execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2016-4223 and CVE-2016-4224. **Reference: CVE-2016-4225**		
Cisco					
Amp Threat Grid Appliance *Cisco AMP Threat Grid Appliance combines advanced malware analysis with deep threat analytics and content in one on-premise appliance.*					
Execute Code	2016-07-12	6.8	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2016-4223 and CVE-2016-4225. **Reference: CVE-2016-4224**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-CIS-AMP T-250716/88
Cloud Network Automation Provisioner *Cisco Cloud Network Automation Provisioner (CNAP) 1.0(0) in Cisco Configuration Assistant (CCA) allows remote attackers to bypass intended filesystem and administrative-endpoint restrictions via GET API calls, aka Bug ID CSCuy77145.*					
Execute Code	2016-07-12	6.8	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2016-4224 and CVE-2016-4225. **Reference: CVE-2016-4223**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-CIS-CLOUD-250716/89
Evolved Programmable Network Manager; Prime Infrastructure *Cisco Evolved Programmable Network Manager provides simplified, converged, multilayer management of carrier-grade networks of all sizes. Prime Infrastructure offers comprehensive lifecycle management of wired/wireless access, campus, and branch networks, rich visibility into end-user connectivity, and application performance assurance.*					
Execute Code	2016-07-12	6.8	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on	https://helpx.adobe.com/security/products/flash-	A-CIS-EVOLV-250716/90

			Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248. **Reference: CVE-2016-4222**	player/apsb16-25.html	
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	7.5	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4221**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-CIS-EVOLV-250716/91
Firesight System Software *Cisco FireSIGHT System Software 5.4.0 through 6.0.1 and ASA with FirePOWER Services 5.4.0 through 6.0.0.1 allow remote attackers to bypass malware protection via crafted fields in HTTP headers, aka Bug ID CSCux22726.*					
Denial of Service; Execute Code; Overflow;	2016-07-12	7.5	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on	https://helpx.adobe.com/security/products/flas	A-CIS-FIRES-250716/92

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

Memory Corruption			Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4220**	h-player/apsb16-25.html	
Meeting Server *Cisco WebEx Meeting Server is a solution bringing the Cisco WebEx conferencing solution; SAAS market leader for many years; into the company private cloud. CWMS has been generating tremendous interest and many deals around the globe from various types of industries and geographical areas.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	7.5	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-CIS-MEETI-250716/93

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

			4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4219**		
Prime Collaboration Provisioning *Cisco Prime Collaboration provides automated and accelerated provisioning, real-time monitoring, proactive troubleshooting, and long-term trending*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	7.5	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4218**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-CIS-PRIME-250716/94
Prime Infrastructure *Prime Infrastructure offers comprehensive lifecycle management of wired/wireless access, campus, and branch*					

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

networks, rich visibility into end-user connectivity, and application performance assurance.					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	7.5	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4217**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-CIS-PRIME-250716/95
Telepresence Video Communication Server; Telepresence Video Communication Server Software *The Cisco TelePresence Video Communication Server simplifies session management and control of telepresence conferences.*					
NA	2016-07-12	5	XMPCore in Adobe XMP Toolkit for Java before 5.1.3 allows remote attackers to read arbitrary files via XML data containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. **Reference: CVE-2016-4216**	https://helpx.adobe.com/security/products/xmpcore/apsb16-24.html	A-CIS-TELEP-250716/96
Web Security Appliance *Cisco Web Security Appliance provides exceptional web security and control for organizations of all sizes integrated into one appliance.*					

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

Bypass	2016-07-12	7.5	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors. **Reference: CVE-2016-4215**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-CIS-WEBS-250716/97
Webex Meetings Server *Bring Cisco WebEx conferencing into your cloud for a highly secure, cost-effective, and flexible collaboration and communications solution.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4214**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-CIS-WEBEX-250716/98
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-CIS-WEBEX-250716/99

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

			15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4213**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-CIS-WEBEX-250716/100

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

			2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4212**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4211**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-CIS-WEBEX-250716/101
Execute Code; Overflow	2016-07-12	7.5	Integer overflow in Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference: CVE-2016-4210**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-CIS-WEBEX-250716/102
Citrix					
Worx Home; Xenmobile Mdx Toolkit *Worx Home is the easiest way to get your work apps and data and to get help when you need it; MDX is the container and management technology used by Citrix XenMobile.*					

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

Execute Code; Overflow	2016-07-12	6.8	Heap-based buffer overflow in Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference: CVE-2016-4209**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-CIT-WORX - 250716/103
Eaton					
Elcsoft *ELCSoft programming software configures all Eaton Logic Control (ELC) controllers. With ELCSoft, applications can be created, edited and monitored.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4208**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-EAT-ELCSO-250716/104
Denial of Service; Execute Code; Overflow; Memory	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic	https://helpx.adobe.com/security/products/acro	A-EAT-ELCSO-250716/105

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

Corruption			before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4207**	bat/apsb16-26.html	
EMC					
Avamar *EMC Avamar is a fast, scalable de-duplication backup and data recovery software and system*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-EMC-AVAMA-250716/106

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

			4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4206**		
Rsa Archer Egrc *RSA Archer Risk Management enables users to proactively address risks to reputation, finances, operations and IT infrastructure as part of a governance, risk management and compliance (GRC) program. The software provides a central GRC management system for identifying risks, evaluating their likelihood of impact and then ties those to mitigating controls and tracks resolution progress.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4205**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-EMC-RSA A-250716/107
Flexerasoftware					
Installanywhere *InstallAnywhere is the multiplatform installation solution of choice to reduce software development time and simplify virtualization.*					

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

Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4204**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-FLE-INSTA-250716/108
Fortinet					
Fortiweb *FortiWeb uses the advanced multi-layered and correlated approach to complete security for your web-based applications in Azure*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195,	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-FOR-FORTI-250716/109

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

			CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4203**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4202**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-FOR-FORTI-250716/110
General Electric					
Cimplicity *CIMPLICITY is a proven automation and control platform, making it the HMI/SCADA choice for many of the world's largest manufacturers.*					
Denial of Service; Execute Code;	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and	https://helpx.adobe.com/securit	A-GEN-CIMPL-250716/111

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

Overflow; Memory Corruption			Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4201**	y/products/acrobat/apsb16-26.html	
Gimp					
Gimp *GIMP (GNU Image Manipulation Program) is a free and open-source raster graphics editor used for image retouching and editing, free-form drawing, resizing, cropping, photo-montages, converting between different image formats, and more specialized tasks.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-GIM-GIMP-250716/112

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

			4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4200**		
Google					
Chrome *Google Chrome is a browser that combines a minimal design with sophisticated technology to make the web faster, safer, and easier.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4199**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-GOO-CHROM-250716/113
HP					
Intelligent Management Center Application Performance Manager; Intelligent Management Center					

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

Branch Intelligent Management System; Intelligent Management Center Endpoint Admission Defense; Intelligent Management Center Network Traffic Analyzer; Intelligent Management Center Platform; Intelligent Management Center User Access Management *HPE Intelligent Management Center Enterprise Software Platform is a comprehensive wired and wireless network management tool supporting the FCAPS model, provides for end-to-end business management of IT, scalability of system architecture, and accommodation of new technology and infrastructure. Intelligent Management Center (IMC) Enterprise Software Platform supports the management of Hewlett Packard Enterprise and third-party devices.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4198**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-HP-INTEL-250716/114
Huawei					
Hisuite *HiSuite allows you to manage Android data and applications.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-HUA-HISUI-250716/115

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

			of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4197**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4196**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-HUA-HISUI-250716/116

Public Cloud Solution

A public cloud is one based on the standard cloud computing model, in which a service provider makes resources,

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

such as applications and storage, available to the general public over the Internet.Public cloud services may be free or offered on a pay-per-usage model.					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4195**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-HUA-PUBLI-250716/117
IBM					
Bigfix Platform *IBM BigFix formerly IBM Endpoint Manager, Tivoli Endpoint Manager (TEM) and before that, BigFix, is a systems-management software product developed by IBM for managing large groups of computers running Windows, Mac OS X, VMware ESX, Linux or UNIX, as well as various mobile operating systems such as Windows Phone, Symbian, iOS and Android.*					

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

Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4194**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-IBM-BIGFI-250716/118
Cognos Analytics *IBM Cognos Analytics offers guided, self-service capabilities designed to solve problems and seize new opportunities quickly.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201,	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-IBM-COGNO-250716/119

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

			CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4193**		
Cognos Business Intelligence *IBM Cognos Business Intelligence is a web-based, integrated business intelligence suite by IBM. It provides a toolset for reporting, analysis, scorecarding, and monitoring of events and metrics. The software consists of several components to meet the different information requirements in a company.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4192**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-IBM-COGNO-250716/120
Denial of Service; Execute Code; Overflow; Memory	2016-07-12	6.8	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and	https://helpx.adobe.com/security/products/acrobat/apsb1	A-IBM-COGNO-250716/121

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

Corruption			Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, and CVE-2016-4254. **Reference: CVE-2016-4191**	6-26.html	
Control Center; Sterling Control Center *IBM Control Center is a centralized monitoring and management system that gives operations personnel the capability to continuously monitor business activities across the enterprise for the following server types: IBM Sterling Connect:Direct, IBM Sterling Connect:Direct File Agent, IBM Sterling Connect:Enterprise, IBM Sterling Connect:Express, IBM QuickFile, IBM Sterling B2B Integrator, IBM Sterling File Gateway, and for many FTP servers. IBM Control Center also allows you to manage the configurations and licenses of Sterling Connect:Direct servers. Sterling Control Center is a system management solution for managing file transfer activity across multiple instances of IBM Sterling Connect:Direct, IBM Sterling Connect:Enterprise, and/or IBM Sterling B2B Integrator.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-CONTR-250716/122

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

			4188, CVE-2016-4189, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4190**		
I Access *IBM i Access is the leading client-to-i connectivity product.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4189**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-I ACC-250716/123
Infosphere Streams; Streams *IBM InfoSphere Streams (referred to as Streams) delivers a highly scalable, agile software infrastructure to perform in-motion analytics on a wide variety of relational and non-relational data types that enter the enterprise at unprecedented volumes and speed, and from thousands of real-time sources. IBM Streams is an advanced analytic*					

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

platform that allows user-developed applications to quickly ingest, analyze and correlate information as it arrives from thousands of data stream sources.					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4188**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-INFOS-250716/124
Integration Bus; Websphere Message Broker *IBM Integration Bus (formerly known as WebSphere Message Broker) is IBM's integration broker from the WebSphere product family that allows business information to flow between disparate applications across multiple hardware and software platforms; IBM WebSphere Message Broker is IBM's integration broker from the WebSphere product family that allows business information to flow between disparate applications across multiple hardware and software platforms.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-INTEG-250716/125

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

			2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4187**		
Jazz Reporting Service *IBM Jazz Reporting Service is an optional component of IBM Rational Reporting for Development Intelligence*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-JAZZ - 250716/126

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

			2016-4246. **Reference: CVE-2016-4186**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4185**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-JAZZ - 250716/127
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-JAZZ - 250716/128

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

			2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4184**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4183**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-JAZZ - 250716/129
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-JAZZ - 250716/130

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

			service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4182**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-JAZZ - 250716/131

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

			2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4181**		
Maximo Asset Management *IBM Maximo Asset Management is an enterprise asset management (EAM) software solution product produced by IBM. It is a solution which enterprises use to track the operation, maintenance and disposal of assets.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4180**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-MAXIM-250716/132
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182,	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-MAXIM-250716/133

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

			CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4179**		
Personal Communications *IBM Personal Communications is a host communication and terminal emulation package for Microsoft Windows that features virtual terminal (VT) Emulation, systems network architecture (SNA) application support, integration and connectivity. Personal Communications is a key component of IBM Host Access Client Package and IBM Host Integration Solution.*					
Bypass; Gain Information	2016-07-12	5	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors. **Reference: CVE-2016-4178**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-PERSO-250716/134
Power Hardware Management Console *A Hardware Management Console (HMC) is an appliance used to manage Power Systems servers.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4176. **Reference: CVE-2016-4177**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-POWER-250716/135
Qradar Security Information And Event Manager *IBM QRadar Security Intelligence Platform provides a unified architecture for integrating security information and*					

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

event management (SIEM), log management, anomaly detection, incident forensics, incident response, and configuration and vulnerability management. It uses an advanced Sense Analytics Engine to detect advanced threats while providing greater ease of use and lower total cost of ownership.					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4177. **Reference: CVE-2016-4176**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-QRADA-250716/136
Qradar Security Information And Event Manager; Security Qradar Incident Forensics *IBM QRadar Security Intelligence Platform provides a unified architecture for integrating security information and event management (SIEM), log management, anomaly detection, incident forensics, incident response, and configuration and vulnerability management. It uses an advanced Sense Analytics Engine to detect advanced threats while providing greater ease of use and lower total cost of ownership. IBM Security QRadar Incident Forensics allows you to quickly and easily conduct in-depth forensics investigations of security incidents.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220,	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-QRADA-250716/137

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

			CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4175**		
Rational Collaborative Lifecycle Management; Rational Team Concert *Colaborative Lifecycle Management is a tightly integrated suite of tools which provides automation for every part of the software development lifecycle from requirements through to testing. Rational Team Concert is a software development team collaboration tool developed by the Rational Software brand of IBM, who first released it in 2008. The software is available in both client versions and a Web version.*					
Execute Code	2016-07-12	6.8	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248. **Reference: CVE-2016-4174**	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-RATIO-250716/138
Security Directory Server; Tivoli Directory Server *IBM Tivoli Directory Server. IBM Security Directory Server is an enterprise directory for corporate intranets and the Internet.Tivoli Directory server is a powerful and authoritative enterprise directory infrastructure that is a critical enabler for enterprise security.*					
Execute Code	2016-07-12	6.8	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-SECUR-250716/139

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

			and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248. **Reference: CVE-2016-4173**		
Security Identity Manager Adapter *Security Identity Manager adapters enable the Security Identity Manager Server to connect to a set of heterogeneous resources.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	10	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239,	https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	A-IBM-SECUR-250716/140

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

			CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246. **Reference: CVE-2016-4172**		
Security Identity Manager Adapter *Security Identity Manager adapters enable the Security Identity Manager Server to connect to a set of heterogeneous resources.*					
Cross Site Request Forgery	2016-07-13	6.8	Cross-site request forgery (CSRF) vulnerability in Fortinet FortiWeb before 5.5.3 allows remote attackers to hijack the authentication of administrators for requests that change the password via unspecified vectors. **Reference: CVE-2016-4066**	http://fortiguard.com/advisory/fortiweb-csrf-vulnerability	A-IBM-SECUR-250716/141
Gain Information	2016-07-03	8.5	The NTP time-server interface on Meinberg IMS-LANTIME M3000, IMS-LANTIME M1000, IMS-LANTIME M500, LANTIME M900, LANTIME M600, LANTIME M400, LANTIME M300, LANTIME M200, LANTIME M100, SyncFire 1100, and LCES devices with firmware before 6.20.004 allows remote authenticated users to obtain root privileges for writing to unspecified scripts, and consequently obtain sensitive information or modify data, by leveraging access to the nobody account. **Reference: CVE-2016-3989**	https://ics-cert.us-cert.gov/advisories/ICSA-16-175-03	A-IBM-SECUR-250716/142
Denial of Service;	2016-07-03	7.5	Multiple stack-based buffer overflows in the	https://ics-cert.us-cert.gov/advisories/IC	A-IBM-SECUR-250716/143

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

Overflow; Gain Information			NTP time-server interface on Meinberg IMS-LANTIME M3000, IMS-LANTIME M1000, IMS-LANTIME M500, LANTIME M900, LANTIME M600, LANTIME M400, LANTIME M300, LANTIME M200, LANTIME M100, SyncFire 1100, and LCES devices with firmware before 6.20.004 allow remote attackers to obtain sensitive information, modify data, or cause a denial of service via a crafted parameter in a POST request. **Reference: CVE-2016-3988**	SA-16-175-03	
Denial of Service; Overflow; Gain Information	2016-07-03	7.5	Stack-based buffer overflow in the NTP time-server interface on Meinberg IMS-LANTIME M3000, IMS-LANTIME M1000, IMS-LANTIME M500, LANTIME M900, LANTIME M600, LANTIME M400, LANTIME M300, LANTIME M200, LANTIME M100, SyncFire 1100, and LCES devices with firmware before 6.20.004 allows remote attackers to obtain sensitive information, modify data, or cause a denial of service via a crafted parameter in a POST request. **Reference: CVE-2016-3962**	https://ics-cert.us-cert.gov/advisories/ICSA-16-175-03	A-IBM-SECUR-250716/144
Security Qradar Incident Forensics *IBM Security QRadar Incident Forensics allows you to quickly and easily conduct in-depth forensics investigations of security incidents.*					

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

Gain Information	2016-07-02	5	The CLI in npm before 2.15.1 and 3.x before 3.8.3, as used in Node.js 0.10 before 0.10.44, 0.12 before 0.12.13, 4 before 4.4.2, and 5 before 5.10.0, includes bearer tokens with arbitrary requests, which allows remote HTTP servers to obtain sensitive information by reading Authorization headers. **Reference: CVE-2016-3956**	http://blog.npmjs.org/post/142036323955/fixing-a-bearer-token-vulnerability	A-IBM-SECUR-250716/145
Tivoli Storage Manager *IBM Spectrum Protect (Tivoli Storage Manager) is a data protection platform that gives enterprises a single point of control and administration for backup and recovery. It is implemented by Anoosha Alla & co It is the flagship product in the IBM Spectrum Protect (Tivoli Storage Manager) family.*					
Denial of Service; Overflow	2016-07-03	10	The usbip_recv_xbuff function in drivers/usb/usbip/usbip_common.c in the Linux kernel before 4.5.3 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted length value in a USB/IP packet. **Reference: CVE-2016-3955**	https://bugzilla.redhat.com/show_bug.cgi?id=1328478	A-IBM-TIVOL-250716/146
Traveler *IBM Traveler is a push mail solution that allows fast access to emaisl, calendars and address books for mobile employees.*					
Denial of Service	2016-07-10	7.1	libc in Android 4.x before 4.4.4 allows remote attackers to cause a denial of service (device hang or reboot) via a crafted file, aka internal bug 28740702. **Reference: CVE-2016-3818**	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-TRAVE-250716/147
Tririga Application Platform *IBM TRIRIGA Application Platform provides a single web-based set of design-time and runtime components.*					

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

Gain Information	2016-07-10	4.3	The MediaTek display driver in Android before 2016-07-05 on Android One devices allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28402240. **Reference: CVE-2016-3816**	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-TRIRI-250716/148
Gain Information	2016-07-10	4.3	The NVIDIA camera driver in Android before 2016-07-05 on Nexus 9 devices allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28522274. **Reference: CVE-2016-3815**	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-TRIRI-250716/149
Gain Information	2016-07-10	4.3	The NVIDIA camera driver in Android before 2016-07-05 on Nexus 9 devices allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28193342. **Reference: CVE-2016-3814**	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-TRIRI-250716/150
Gain Information	2016-07-10	4.3	The Qualcomm USB driver in Android before 2016-07-05 on Nexus 5, 5X, 6, and 6P devices allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28172322 and Qualcomm internal bug CR1010222. **Reference: CVE-2016-3813**	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-TRIRI-250716/151
Urbancode Deploy *IBM UrbanCode Deploy is a tool for automating application deployments through your environments.*					
Gain Information	2016-07-10	4.3	The MediaTek video codec driver in Android before 2016-07-05 on Android One devices	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-URBAN-250716/152

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

			allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28174833 and MediaTek internal bug ALPS02688832. **Reference: CVE-2016-3812**		
Watson Developer Cloud *The Watson Developer Cloud is a library of Watson APIs that you can use to create Powered by Watson apps.*					
Gain Privileges	2016-07-10	9.3	The kernel video driver in Android before 2016-07-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 28447556. **Reference: CVE-2016-3811**	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-WATSO-250716/153
Websphere Application Server *WebSphere Application Server (WAS) is a software product that performs the role of a web application server. More specifically, it is a software framework and middleware that hosts Java based web applications. It is the flagship product within IBM's WebSphere software suite.*					
Gain Information	2016-07-10	4.3	The MediaTek Wi-Fi driver in Android before 2016-07-05 on Android One devices allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28175522 and MediaTek internal bug ALPS02694389. **Reference: CVE-2016-3810**	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-WEBSP-250716/154
Gain Information	2016-07-10	4.3	The networking component in Android before 2016-07-05 on Android One, Nexus 5, Nexus 5X, Nexus 6, Nexus 6P, Nexus 7 (2013), Nexus 9, Nexus Player, and Pixel C devices allows attackers to obtain sensitive information via a crafted application, aka internal bug 27532522.	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-WEBSP-250716/155

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-2016-3809		
Gain Privileges	2016-07-10	9.3	The serial peripheral interface driver in Android before 2016-07-05 on Pixel C devices allows attackers to gain privileges via a crafted application, aka internal bug 28430009. **Reference: CVE-2016-3808**	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-WEBSP-250716/156
Gain Privileges	2016-07-10	9.3	The serial peripheral interface driver in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 28402196. **Reference: CVE-2016-3807**	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-WEBSP-250716/157
Websphere Commerce *IBM WebSphere Commerce AKA WCS (WebSphere Commerce Suite) is a software platform framework for e-commerce, including marketing, sales, customer and order processing functionality in a tailorable, integrated package.*					
Gain Privileges	2016-07-10	9.3	The MediaTek display driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28402341 and MediaTek internal bug ALPS02715341. **Reference: CVE-2016-3806**	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-WEBSP-250716/158
Gain Privileges	2016-07-10	9.3	The MediaTek power management driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28333002 and MediaTek internal bug ALPS02694412.	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-WEBSP-250716/159

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-2016-3805		
Websphere Extreme Scale *IBM WebSphere eXtreme Scale is an elastic, scalable, in-memory data grid (IMDG). With WebSphere eXtreme Scale, you can expect an enhanced quality of service in high-performance computing environments*					
Gain Privileges	2016-07-10	9.3	The MediaTek power management driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28332766 and MediaTek internal bug ALPS02694410. **Reference: CVE-2016-3804**	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-WEBSP-250716/160
Gain Privileges	2016-07-10	9.3	The kernel filesystem implementation in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 28588434. **Reference: CVE-2016-3803**	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-WEBSP-250716/161
IBM; Nodejs; NPM					
SDK; Node.js; NPM *A software development kit (SDK or "devkit") is typically a set of software development tools that allows the creation of applications for a certain software package, software framework, hardware platform, computer system, video game console, operating system, or similar development platform. In software development, Node.js is an open-source, cross-platform runtime environment for developing server-side Web applications. NPM is a command-line tool for interacting with a huge repository of Node.js projects.*					
Gain Privileges	2016-07-10	9.3	The kernel filesystem implementation in Android before 2016-07-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 28271368. **Reference: CVE-2016-3802**	http://source.android.com/security/bulletin/2016-07-01.html	A-IBM-SDK; -250716/162
Invisionpower					
Invision Power Board, PHP *IP Board is an Internet forum software produced by Invision Power Services, Inc. PHP is a general-purpose scripting language that is especially suited to server-side web development, in which case PHP generally runs on a web server. Any PHP code in a requested file is executed by the PHP runtime, usually to create dynamic web page content or dynamic images used on websites or elsewhere.*					
Gain Privileges	2016-07-10	9.3	The MediaTek GPS driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka	http://source.android.com/security/bulletin/2016-07-01.html	A-INV-INVIS-250716/163

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

			Android internal bug 28174914 and MediaTek internal bug ALPS02688853. **Reference: CVE-2016-3801**		
ISC					
Bind *BIND is open source software that implements the Domain Name System (DNS) protocols for the Internet.*					
Gain Privileges	2016-07-10	9.3	The MediaTek video driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28175027 and MediaTek internal bug ALPS02693739. **Reference: CVE-2016-3800**	http://source.android.com/security/bulletin/2016-07-01.html	A-ISC-BIND-250716/164
Linecorp					
Line; Line Installer *LINE is a new communication app which allows you to make FREE voice calls and send FREE messages whenever and wherever you are, 24 hours a day. Line installers and repairers often work in teams to install and fix cables and wires.*					
Gain Privileges	2016-07-10	9.3	The MediaTek video driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28175025 and MediaTek internal bug ALPS02693738. **Reference: CVE-2016-3799**	http://source.android.com/security/bulletin/2016-07-01.html	A-LIN-LINE-250716/165
Microfocus					
Rumba *Rumba is a terminal emulation solution with UI (User Interface) modernization properties.*					
Gain Privileges	2016-07-10	9.3	The MediaTek hardware sensor driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28174490 and MediaTek internal bug ALPS02703105. **Reference: CVE-2016-3798**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-RUMBA-250716/166
Gain Privileges	2016-07-10	9.3	The Qualcomm Wi-Fi driver in Android before 2016-07-05 on Nexus 5X devices allows attackers to gain privileges via a crafted application, aka Android internal bug	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-RUMBA-250716/167

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

			28085680 and Qualcomm internal bug CR1001450. **Reference: CVE-2016-3797**		
Microsoft					
.net Framework *The .NET Framework helps you create mobile, desktop, and web applications that run on Windows PCs, devices and servers and it's included in Visual Studio.*					
Gain Privileges	2016-07-10	9.3	The MediaTek power driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 29008443 and MediaTek internal bug ALPS02677244. **Reference: CVE-2016-3796**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-.NET - 250716/168
Edge *Microsoft Edge (formerly Project Spartan) is the name of Microsoft's next-generation web browser built into Windows 10.*					
Gain Privileges	2016-07-10	9.3	The MediaTek power driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28085222 and MediaTek internal bug ALPS02677244. **Reference: CVE-2016-3795**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-EDGE-250716/169
Gain Privileges	2016-07-10	9.3	The NVIDIA camera driver in Android before 2016-07-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28026625. **Reference: CVE-2016-3793**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-EDGE-250716/170
Gain Privileges	2016-07-10	9.3	CORE/HDD/src/wlan_hdd_hostapd.c in the Qualcomm Wi-Fi driver in Android before 2016-07-05 on Nexus 7 (2013) devices mishandles userspace data copying, which allows attackers to gain privileges via a crafted application, aka Android internal bug 27725204 and Qualcomm internal bug CR561022. **Reference: CVE-2016-3792**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-EDGE-250716/171
Gain Privileges	2016-07-10	9.3	The kernel filesystem implementation in Android	http://source.android.com/secur	A-MIC-EDGE-250716/172

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

			before 2016-07-05 on Nexus 5X, Nexus 6, Nexus 6P, Nexus Player, and Pixel C devices allows attackers to gain privileges via a crafted application, aka internal bug 28588279. **Reference: CVE-2016-3775**	ity/bulletin/2016-07-01.html	
Gain Privileges	2016-07-10	9.3	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 29008609 and MediaTek internal bug ALPS02703102. **Reference: CVE-2016-3774**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-EDGE-250716/173
Edge; Internet Explorer *Microsoft Edge (formerly Project Spartan) is the name of Microsoft's next-generation web browser built into Windows 10. Internet Explorer is a discontinued series of graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating systems, starting in 1995.*					
Gain Privileges	2016-07-10	9.3	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 29008363 and MediaTek internal bug ALPS02703102. **Reference: CVE-2016-3773**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-EDGE;-250716/174
Gain Privileges	2016-07-10	9.3	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 29008188 and MediaTek internal bug ALPS02703102. **Reference: CVE-2016-3772**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-EDGE;-250716/175
Gain Privileges	2016-07-10	9.3	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 29007611 and MediaTek internal bug ALPS02703102. **Reference: CVE-2016-3771**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-EDGE;-250716/176
Gain Privileges	2016-07-10	9.3	The MediaTek drivers in Android before 2016-07-05 on	http://source.android.com/secur	A-MIC-EDGE;-250716/177

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

			Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 28346752 and MediaTek internal bug ALPS02703102. **Reference: CVE-2016-3770**	ity/bulletin/2016-07-01.html	
Gain Privileges	2016-07-10	9.3	The NVIDIA video driver in Android before 2016-07-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28376656. **Reference: CVE-2016-3769**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-EDGE;-250716/178
Gain Privileges	2016-07-10	9.3	The Qualcomm performance component in Android before 2016-07-05 on Nexus 5, 6, 5X, 6P, and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28172137 and Qualcomm internal bug CR1010644. **Reference: CVE-2016-3768**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-EDGE;-250716/179
Gain Privileges	2016-07-10	9.3	The MediaTek Wi-Fi driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28169363 and MediaTek internal bug ALPS02689526. **Reference: CVE-2016-3767**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-EDGE;-250716/180
Excel; Excel Rt; Office; Office Web Apps; Powerpoint; Powerpoint Rt; Sharepoint Server; Word; Word Rt *Microsoft Office is an office suite of applications, servers, and services developed by Microsoft. Windows RT is a version of Windows 8 that runs on devices (mainly tablets) that use ARM processors rather than Intel processors.*					
Denial of Service	2016-07-10	7.8	MPEG4Extractor.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 does not check whether memory allocation succeeds, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted file, aka internal bug 28471206.	https://android.googlesource.com/platform/frameworks/av/+/e7142a0703bc93f75e213e96ebc19000022afed9	A-MIC-EXCEL-250716/181

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-2016-3766		
Excel; Excel for Mac; Excel Rt; Excel Viewer; Office Compatibility Pack *Microsoft Office is an office suite of applications, servers, and services developed by Microsoft; Windows RT is a version of Windows 8 that runs on devices (mainly tablets) that use ARM processors rather than Intel processors; Excel 2016 for Mac brings lots of welcome improvements to the workhorse spreadsheet but also leaves out useful tools; Excel Viewer is a software designed by Microsoft. Its main function is to open and print Excel workbooks even though there is no Excel Office installed on the computer; Microsoft Office Compatibility Pack is an add-on for Microsoft Office 2000, Office XP and Office 2003 to open, edit and save Microsoft's newer Word, Excel and Powerpoint formats that were introduced with Office 2007. The tool also adds support to the 2003 versions of Word Viewer, Excel Viewer and Powerpoint Viewer to open DOCX, DOCM, XSLX and PPTX files.*					
Denial of Service; Gain Information	2016-07-10	6.4	decoder/impeg2d_bitstream.c in mediaserver in Android 6.x before 2016-07-01 allows attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted application, aka internal bug 28168413. **Reference: CVE-2016-3765**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-EXCEL-250716/182
Internet Explorer *Internet Explorer is a discontinued series of graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating systems, starting in 1995*					
Gain Information	2016-07-10	5	media/libmediaplayerservice/MetadataRetrieverClient.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows attackers to obtain sensitive pointer information via a crafted application, aka internal bug 28377502. **Reference: CVE-2016-3764**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-INTER-250716/183
NA	2016-07-10	5	net/PacProxySelector.java in the Proxy Auto-Config (PAC) feature in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 does not ensure that URL information is restricted to a scheme, host, and port, which allows remote attackers to discover credentials by operating a server with a PAC script, aka internal bug 27593919. **Reference: CVE-2016-3763**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-INTER-250716/184

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

Gain Privileges	2016-07-10	9.3	The sockets subsystem in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows attackers to gain privileges via a crafted application that uses (1) the AF_MSM_IPC socket class or (2) another socket class that is unrecognized by SELinux, aka internal bug 28612709. **Reference: CVE-2016-3762**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-INTER-250716/185
Gain Information	2016-07-10	2.1	NfcService.java in NFC in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows attackers to obtain sensitive foreground-application information via a crafted background application, aka internal bug 28300969. **Reference: CVE-2016-3761**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-INTER-250716/186
Gain Privileges	2016-07-10	5.4	Bluetooth in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows local users to gain privileges by establishing a pairing that remains present during a session of the primary user, aka internal bug 27410683. **Reference: CVE-2016-3760**	https://android.googlesource.com/platform/system/bt/+/37c88107679d36c419572732b4af6e18bb2f7dce	A-MIC-INTER-250716/187
Gain Information	2016-07-10	5	The Framework APIs in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allow attackers to read backup data via a crafted application that leverages priv-app access to insert a backup transport, aka internal bug 28406080. **Reference: CVE-2016-3759**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-INTER-250716/188
Overflow; Gain Privileges	2016-07-10	9.3	Multiple buffer overflows in libdex/OptInvocation.cpp in DexClassLoader in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allow attackers to gain privileges via a crafted application that	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-INTER-250716/189

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

			provides a long filename, aka internal bug 27840771. **Reference: CVE-2016-3758**		
Gain Privileges	2016-07-10	5.9	The print_maps function in toolbox/lsof.c in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows user-assisted attackers to gain privileges via a crafted application that attempts to list a long name of a memory-mapped file, aka internal bug 28175237. NOTE: print_maps is not related to the Vic Abell lsof product. **Reference: CVE-2016-3757**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-INTER-250716/190
Office; Office Compatibility Pack; Word; Word For Mac; Word Rt; Word Viewer *Microsoft Office is an office suite of applications, servers, and services developed by Microsoft. Windows RT is a version of Windows 8 that runs on devices (mainly tablets) that use ARM processors rather than Intel processors. Windows RT provides the Metro portion of Windows 8 and a custom version of Office 2013; it does not run standard Windows software. Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services. Office Online (previously Office Web Apps) is an online office suite offered by Microsoft, which allows users to create and edit files using lightweight, web browser-based versions of Microsoft Office applications: Word, Excel, PowerPoint and OneNote. Microsoft Office Compatibility Pack is an add-on for Microsoft Office 2000, Office XP and Office 2003 to open, edit and save Microsoft's newer Word, Excel and Powerpoint formats that were introduced with Office 2007. The tool also adds support to the 2003 versions of Word Viewer, Excel Viewer and Powerpoint Viewer to open DOCX, DOCM, XSLX and PPTX files.*					
Denial of Service	2016-07-10	7.8	Tremolo/res012.c in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 does not validate the number of partitions, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 28556125. **Reference: CVE-2016-3756**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-OFFIC-250716/191
Denial of Service	2016-07-10	7.8	decoder/ih264d_parse_pslice.c in mediaserver in Android 6.x before 2016-07-01 does not properly select concealment frames, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 28470138.	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-OFFIC-250716/192

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-2016-3755		
Office; Office Web Apps; Sharepoint Server; Word; Word For Mac; Word Rt *Microsoft Office is an office suite of applications, servers, and services developed by Microsoft. Windows RT is a version of Windows 8 that runs on devices (mainly tablets) that use ARM processors rather than Intel processors. Windows RT provides the Metro portion of Windows 8 and a custom version of Office 2013; it does not run standard Windows software. Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services. Office Online (previously Office Web Apps) is an online office suite offered by Microsoft, which allows users to create and edit files using lightweight, web browser-based versions of Microsoft Office applications: Word, Excel, PowerPoint and OneNote. Microsoft Office Compatibility Pack is an add-on for Microsoft Office 2000, Office XP and Office 2003 to open, edit and save Microsoft's newer Word, Excel and Powerpoint formats that were introduced with Office 2007. The tool also adds support to the 2003 versions of Word Viewer, Excel Viewer and Powerpoint Viewer to open DOCX, DOCM, XSLX and PPTX files.*					
Denial of Service	2016-07-10	7.8	mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 does not limit process-memory usage, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 28615448. **Reference: CVE-2016-3754**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-OFFIC-250716/193
Outlook; Outlook Rt *Microsoft Outlook is a personal information manager from Microsoft, available as a part of the Microsoft Office suite. Although often used mainly as an email application, it also includes a calendar, task manager, contact manager, note taking, journal, and web browsing. Outlook 2013 RT is visually the same when compared to the regular Outlook 2013 application but is optimized for the ARM processor, has Touch Mode enabled by default and contains various other battery life increasing and disk space usage reducing changes.*					
Gain Information	2016-07-10	5	mediaserver in Android 4.x before 4.4.4 allows remote attackers to obtain sensitive information via unspecified vectors, aka internal bug 27210135. **Reference: CVE-2016-3753**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-OUTLO-250716/194
Word Viewer *After installing Word Viewer you can open and view DOC files without having to use Microsoft Office Word.*					
Gain Privileges	2016-07-10	7.5	internal/app/ChooserActivity.java in the ChooserTarget service in Android 6.x before 2016-07-01 mishandles target security checks, which allows attackers to gain privileges via a crafted application, aka internal bug 28384423. **Reference: CVE-2016-3752**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIC-WORD -250716/195
Libbpg *libbpg is a library for the BPG graphics format.*					

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

Gain Privileges	2016-07-10	7.5	Unspecified vulnerability in libpng before 1.6.20, as used in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01, allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 23265085. **Reference: CVE-2016-3751**	http://source.android.com/security/bulletin/2016-07-01.html	A-MIR-LIBBP-250716/196
Moxa					
Device Server Web Console 5232-n Firmware *Moxa Device Server Web Console 5232-N allows remote attackers to bypass authentication, and consequently modify settings and data, via vectors related to reading a cookie parameter containing a UserId value.*					
Bypass	2016-07-10	7.5	libs/binder/Parcel.cpp in the Parcels Framework APIs in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 does not validate the return value of the dup system call, which allows attackers to bypass an isolation protection mechanism via a crafted application, aka internal bug 28395952. **Reference: CVE-2016-3750**	http://source.android.com/security/bulletin/2016-07-01.html	A-MOX-DEVIC-250716/197
Mgate Mb3170, Mb3180, Mb3270, Mb3280, Mb3480, Router Firmware *The MB3180, MB3280, and MB3480 are standard Modbus gateways that convert between Modbus TCP and Modbus RTU/ASCII protocols. Up to 16 simultaneous Modbus TCP masters are supported, with up to 31 RTU/ASCII slaves per serial port. For RTU/ASCII masters, up to 32 TCP slaves are supported. The MGate MB3170 and MB3270 are 1 and 2-port Modbus gateways, respectively, that convert between Modbus TCP, ASCII, and RTU communication protocols.*					
NA	2016-07-10	4.6	server/LockSettingsService.java in LockSettingsService in Android 6.x before 2016-07-01 allows attackers to modify the screen-lock password or pattern via a crafted application, aka internal bug 28163930. **Reference: CVE-2016-3749**	http://source.android.com/security/bulletin/2016-07-01.html	A-MOX-MGATE-250716/198
NTP					
NTP *Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use.*					

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

Bypass	2016-07-10	7.5	The sockets subsystem in Android 6.x before 2016-07-01 allows attackers to bypass intended system-call restrictions via a crafted application that makes an ioctl call, aka internal bug 28171804. **Reference: CVE-2016-3748**	http://source.android.com/security/bulletin/2016-07-01.html	A-NTP-NTP-250716/199
Gain Privileges	2016-07-10	10	Use-after-free vulnerability in the mm-video-v4l2 venc component in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27903498. **Reference: CVE-2016-3747**	http://source.android.com/security/bulletin/2016-07-01.html	A-NTP-NTP-250716/200
Gain Privileges	2016-07-10	7.5	Use-after-free vulnerability in the mm-video-v4l2 vdec component in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27890802. **Reference: CVE-2016-3746**	http://source.android.com/security/bulletin/2016-07-01.html	A-NTP-NTP-250716/201
Overflow; Gain Privileges	2016-07-10	7.5	Multiple buffer overflows in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allow attackers to gain privileges via a crafted application that provides an AudioEffect reply, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 28173666. **Reference: CVE-2016-3745**	http://source.android.com/security/bulletin/2016-07-01.html	A-NTP-NTP-250716/202
Overflow; Gain Privileges	2016-07-10	4.3	Buffer overflow in the create_pbuf function in btif/src/btif_hh.c in Bluetooth	http://source.android.com/security/bulletin/201	A-NTP-NTP-250716/203

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

			in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows remote attackers to gain privileges via a crafted pairing operation, aka internal bug 27930580. **Reference: CVE-2016-3744**	6-07-01.html	
Openvswitch; Redhat					
Openvswitch, Openshift *Open vSwitch, sometimes abbreviated as OVS, is a production-quality open-source implementation of a distributed virtual multilayer switch. OpenShift is an open source PaaS by Red Hat based on top of Docker containers and the Kubernetes container cluster manager for enterprise app development*					
Denial of Service; Execute Code; Memory Corruption	2016-07-10	7.5	decoder/ih264d_api.c in mediaserver in Android 6.x before 2016-07-01 does not initialize certain data structures, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 27907656. **Reference: CVE-2016-3743**	http://source.android.com/security/bulletin/2016-07-01.html	A-OPE-OPENV-250716/204
Phpmyadmin					
Phpmyadmin *phpMyAdmin is a free and open source tool written in PHP intended to handle the administration of MySQL or MariaDB with the use of a web browser.*					
Denial of Service; Execute Code; Memory Corruption	2016-07-10	7.5	decoder/ih264d_process_intra_mb.c in media server in Android 6.x before 2016-07-01 mishandles intra mode, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28165659. **Reference: CVE-2016-3742**	http://source.android.com/security/bulletin/2016-07-01.html	A-PHP-PHPMY-250716/205
Denial of Service; Execute Code; Memory Corruption	2016-07-10	7.5	The H.264 decoder in mediaserver in Android 6.x before 2016-07-01 does not initialize certain slice data, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28165661.	http://source.android.com/security/bulletin/2016-07-01.html	A-PHP-PHPMY-250716/206

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-2016-3741		
Bypass	2016-07-12	2.1	Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to bypass the Secure Boot protection mechanism by leveraging administrative access to install a crafted policy, aka "Secure Boot Security Feature Bypass." **Reference: CVE-2016-3287**	http://technet.microsoft.com/en-us/security/bulletin/ms16-094	A-PHP-PHPMY-250716/207
Gain Privileges	2016-07-12	7.2	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3249, CVE-2016-3252, and CVE-2016-3254. **Reference: CVE-2016-3286**	http://technet.microsoft.com/en-us/security/bulletin/ms16-090	A-PHP-PHPMY-250716/208
Rexroth					
Bladecontrol-webvis *BLADEcontrol continuously monitors the condition of rotor blades to detect early signs of damage to the blades and prevent greater problems. Blade lifetime is thereby extended significantly.*					
Execute Code; Overflow; Memory Corruption	2016-07-12	9.3	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-3284**	http://technet.microsoft.com/en-us/security/bulletin/ms16-088	A-REX-BLADE-250716/209
Execute Code; Overflow; Memory Corruption	2016-07-12	9.3	Microsoft Word Viewer allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory	http://technet.microsoft.com/en-us/security/bulletin/ms16-088	A-REX-BLADE-250716/210

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

			Corruption Vulnerability." **Reference: CVE-2016-3283**		
Samba					
Samba *Samba is a free software re-implementation of the SMB/CIFS networking protocol, and was originally developed by Andrew Tridgell.*					
Execute Code; Overflow; Memory Corruption	2016-07-12	9.3	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, SharePoint Server 2016, Office Web Apps 2010 SP2, Office Web Apps Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-3282**	http://technet.microsoft.com/en-us/security/bulletin/ms16-088	A-SAM-SAMBA-250716/211
Siemens					
Sicam Pas *SICAM PAS is an energy automation solution. Its system architecture makes it scalable.*					
Execute Code; Overflow; Memory Corruption	2016-07-12	9.3	Microsoft Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-3281**	http://technet.microsoft.com/en-us/security/bulletin/ms16-088	A-SIE-SICAM-250716/212
Execute Code; Overflow; Memory Corruption	2016-07-12	9.3	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word for Mac 2011, Word 2016 for Mac,	http://technet.microsoft.com/en-us/security/bulletin/ms16-088	A-SIE-SICAM-250716/213

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

			Office Compatibility Pack SP3, and Word Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-3280**		
Symantec					
Workspace Streaming; Workspace Virtualization *Symantec's Endpoint Virtualization Suite addresses the growing need to contain the high cost and complexity associated with managing endpoints today, while simultaneously insuring maximum end user productivity. Greater user mobility, adoption of multiple compute models, and proliferation of various virtualization technologies all contribute to the growing conflict between IT costs and end user flexibility. Symantec Endpoint Virtualization Suite offers products to improve both sides of that equation for all users. Symantec Workspace Streaming and Symantec Workspace Virtualization are a powerful and robust set of solutions within the suite giving an enterprise the ability to package, deliver and manage the lifecycle of applications.*					
Execute Code	2016-07-12	4.3	Microsoft Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Word 2010 SP2, Excel 2013 SP1, PowerPoint 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, PowerPoint 2013 RT SP1, Word 2013 RT SP1, Excel 2016, Word 2016, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to execute arbitrary code via a crafted XLA file, aka "Microsoft Office Remote Code Execution Vulnerability." **Reference: CVE-2016-3279**	http://technet.microsoft.com/en-us/security/bulletin/ms16-088	A-SYM-WORKS-250716/214
Execute Code; Overflow; Memory Corruption	2016-07-12	9.3	Microsoft Outlook 2010 SP2, 2013 SP1, 2013 RT SP1, and 2016 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-3278**	http://technet.microsoft.com/en-us/security/bulletin/ms16-088	A-SYM-WORKS-250716/215
Tollgrade					
Lighthouse Sms *LightHouse Sensor Management System (SMS) software classifies power disturbance events and provides the visualization and situational awareness needed to quickly respond to load planning, outages, and faults. An easy-to-use software management tool, SMS is designed to simplify remote management and configuration of sensors. In addition, it combines predictive analytics features including fault event classification, load logging, reporting and graphing of data, alarms, and waveforms capture for analysis.*					

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

Gain Information	2016-07-12	2.6	Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability." **Reference: CVE-2016-3277**	http://technet.microsoft.com/en-us/security/bulletin/ms16-085	A-TOL-LIGHT-250716/216
NA	2016-07-12	2.6	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to conduct content-spoofing attacks via a crafted URL, aka "Microsoft Browser Spoofing Vulnerability." **Reference: CVE-2016-3276**	http://technet.microsoft.com/en-us/security/bulletin/ms16-085	A-TOL-LIGHT-250716/217
Vmware					
Nsx Edge; Vcloud Networking And Security Edge *NSX Edge provides network edge security and gateway services to isolate a virtualized network. You can install an NSX Edge either as a logical (distributed) router or as a services gateway. VMware vCloud Networking and Security solves the data center challenges by virtualizing networks and security to create efficient, agile, extensible logical constructs that meet the performance and scale requirements of virtualized datacenters.*					
	2016-07-12	2.6	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to conduct content-spoofing attacks via a crafted URL, aka "Microsoft Browser Spoofing Vulnerability." **Reference: CVE-2016-3274**	http://technet.microsoft.com/en-us/security/bulletin/ms16-085	A-VMW-NSX E-250716/218
Vcenter Server *vCenter server is installed on WindowsServer or Linux Server. VMware vCenter server is a centralized management application that lets you manage virtual machines and ESXi hosts centrally. vSphere client is used to access vCenter Server and ultimately manage ESXi servers.*					
Cross Site Scripting; Gain Information	2016-07-12	2.6	The XSS Filter in Microsoft Internet Explorer 9 through 11 and Microsoft Edge does not properly restrict JavaScript code, which allows remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability." **Reference: CVE-2016-3273**	http://technet.microsoft.com/en-us/security/bulletin/ms16-085	A-VMW-VCENT-250716/219
Vrealize Log Insight *Log Insight gives administrators the ability to consolidate logs, monitor and troubleshoot vSphere and to perform security auditing and compliance testing.*					

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

Gain Information	2016-07-12	2.1	The kernel in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandles page-fault system calls, which allows local users to obtain sensitive information from an arbitrary process via a crafted application, aka "Windows Kernel Information Disclosure Vulnerability." **Reference: CVE-2016-3272**	http://technet.microsoft.com/en-us/security/bulletin/ms16-092	A-VMW-VREAL-250716/220
Vrealize Log Insight *Log Insight gives administrators the ability to consolidate logs, monitor and troubleshoot vSphere and to perform security auditing and compliance testing.*					
Gain Information	2016-07-12	4.3	The VBScript engine in Microsoft Edge allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Scripting Engine Information Disclosure Vulnerability." **Reference: CVE-2016-3271**	http://technet.microsoft.com/en-us/security/bulletin/ms16-085	A-VMW-VREAL-250716/221
Wecon					
Levistudio *LeviStudio is an HMI programming software.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	9.3	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3265. **Reference: CVE-2016-3269**	http://technet.microsoft.com/en-us/security/bulletin/ms16-085	A-WEC-LEVIS-250716/222
Levistudio *LeviStudio is an HMI programming software.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	9.3	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than	http://technet.microsoft.com/en-us/security/bulletin/ms16-085	A-WEC-LEVIS-250716/223

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

			CVE-2016-3269. **Reference: CVE-2016-3265**		
Application/Operating System (A/OS)					
Apache; Canonical; Debian					
Commons Fileupload; Tomcat;Ubuntu Linux; Debian Linux *The Commons FileUpload package makes it easy to add robust, high-performance, file upload capability to your servlets and web applications. Apache Tomcat, often referred to as Tomcat, is an open-source web server developed by the Apache Software Foundation (ASF); Ubuntu is a Debian-based Linux operating system and distribution for personal computers, smartphones and network servers; Debian is a popular and freely-available computer operating system that uses the Linux kernel and other program components obtained from the GNU project; Debian can be downloaded over the Internet or, for a small charge, obtained on CD.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	7.6	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability." **Reference: CVE-2016-3264**	http://technet.microsoft.com/en-us/security/bulletin/ms16-085	A-O-APA-COMMO-250716/224
Apache; Debian					
Xerces-c++; Debian Linux *Xerces-C++ is a validating XML parser written in a portable subset of C++. Xerces-C++ makes it easy to give your application the ability to read and write XML data. A shared library is provided for parsing, generating, manipulating, and validating XML documents using the DOM, SAX, and SAX2 APIs; Debian is a popular and freely-available computer operating system that uses the Linux kernel and other program components obtained from the GNU project; Debian can be downloaded over the Internet or, for a small charge, obtained on CD.*					
Gain Information	2016-07-12	2.6	Microsoft Internet Explorer 11 allows remote attackers to obtain sensitive information via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability." **Reference: CVE-2016-3261**	http://technet.microsoft.com/en-us/security/bulletin/ms16-084	A-O-APA-XERCE-250716/225
Canonical; Debian; Libreoffice					
Libreoffice; Debian Linux; Ubuntu Linux *LibreOffice is the free power-packed Open Source personal productivity suite for Windows, Macintosh and Linux, that gives you six feature-rich applications for all your document production and data processing needs; Debian is a popular and freely-available computer operating system that uses the Linux kernel and other program components obtained from the GNU project. Debian can be downloaded over the Internet or, for a small charge, obtained on CD; Ubuntu is a Debian-based Linux operating system and distribution for personal computers, smartphones and network servers*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	9.3	The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Internet Explorer 11, Microsoft Edge, and other	http://technet.microsoft.com/en-us/security/bulletin/ms16-085	A-O-CAN-LIBRE-250716/226

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

			products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." **Reference: CVE-2016-3260**		
Cisco					
Adaptive Security Appliance Software *Cisco ASA Software delivers enterprise-class security capabilities for the ASA security family in a variety of form factors.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	9.3	The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Internet Explorer 9 through 11, Microsoft Edge, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3248. **Reference: CVE-2016-3259**	http://technet.microsoft.com/en-us/security/bulletin/ms16-085	A-O-CIS-ADAPT-250716/227
Debian, Redhat					
Debian Linux; Libvirt *Debian is a popular and freely-available computer operating system that uses the Linux kernel and other program components obtained from the GNU project. Debian can be downloaded over the Internet or, for a small charge, obtained on CD; libvirt is an open source API, daemon and management tool for managing platform virtualization.*					
Bypass	2016-07-12	1.2	Race condition in the kernel in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to bypass the Low Integrity protection mechanism and write to files by leveraging unspecified object-manager features, aka "Windows File System Security Feature Bypass." **Reference: CVE-2016-3258**	http://technet.microsoft.com/en-us/security/bulletin/ms16-092	A-O-DEB-DEBIA-250716/228
Debian; Openstack; Redhat					
Debian Linux; Horizon; Openstack *Debian is a popular and freely-available computer operating system that uses the Linux kernel and other program components obtained from the GNU project. Debian can be downloaded over the Internet or, for a small charge,*					

obtained on CD;Horizon Software is an innovative leader in technology for food service operations and online payments, offering scalable solutions capable of meeting the needs and budget of any operation; OpenStack is a free and open-source software platform for cloud computing, mostly deployed as an infrastructure-as-a-service (IaaS).					
Bypass; Gain Information	2016-07-12	2.1	Microsoft Windows 10 Gold and 1511 allows local users to bypass the Secure Kernel Mode protection mechanism and obtain sensitive information via a crafted application, aka "Windows Secure Kernel Mode Information Disclosure Vulnerability." **Reference: CVE-2016-3256**	http://technet.microsoft.com/en-us/security/bulletin/ms16-089	A-O-DEB-DEBIA-250716/229
Fedoraproject; Graphicsmagick; suse					
Fedora; Graphicsmagick; Linux Enterprise Debuginfo; Linux Enterprise Software Development Kit; Studio Onsite *Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat. Fedora contains software distributed under a free and open-source license and aims to be on the leading edge of such technologies; GraphicsMagick is the swiss army knife of image processing. Comprised of 267K physical lines (according to David A. Wheeler's SLOCCount) of source code in the base package (or 1,225K including 3rd party libraries) it provides a robust and efficient collection of tools and libraries which support reading, writing, and manipulating an image in over 88 major formats including important formats like DPX, GIF, JPEG, JPEG-2000, PNG, PDF, PNM, and TIFF; Red Hat Enterprise Linux also provides -debuginfo packages for all architecture-dependent RPMs included in the operating system; SUSE Linux Enterprise 10 Software Developer Kit (SDK) is a comprehensive development toolkit that is designed to support developers, as well as independent hardware vendors (IHVs) and independent software vendors (ISVs), to create applications on or port them to SUSE Linux Enterprise 10 products; SUSE Studio Onsite is a Web application for building and testing appliances in a Web browser.*					
Gain Information	2016-07-12	5	Microsoft .NET Framework 2.0 SP2, 3.5, 3.5.1, 4.5.2, 4.6, and 4.6.1 allows remote attackers to read arbitrary files via XML data containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, aka ".NET Information Disclosure Vulnerability." **Reference: CVE-2016-3255**	http://technet.microsoft.com/en-us/security/bulletin/ms16-091	A-O-FED-FEDOR-250716/230
Fedoraproject; Pivotal Software					
Fedora; Spring Framework *Fedora is a linux based operating system; The Spring Framework is an application framework and inversion of control container for the Java platform.*					
Gain Privileges	2016-07-12	7.2	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server	http://technet.microsoft.com/en-us/security/bulletin/ms16-090	A-O-FED-FEDOR-250716/231

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

			2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3249, CVE-2016-3252, and CVE-2016-3286. **Reference: CVE-2016-3254**		
KDE; Novell					
Kde Frameworks; Leap; Opensuse *KDE Frameworks is a collection of libraries and software frameworks by KDE that serve as technological foundation for KDE Plasma 5 and KDE Applications distributed under the GNU Lesser General Public License (LGPL); LEAP Legal Software provides a completely integrated Legal Case Management & Legal Accounting Solutionp; The openSUSE project is a worldwide effort that promotes the use of Linux .*					
Gain Privileges	2016-07-12	7.2	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3249, CVE-2016-3254, and CVE-2016-3286. **Reference: CVE-2016-3252**	http://technet.microsoft.com/en-us/security/bulletin/ms16-090	A-O-KDE-KDEF-250716/232
Microsoft, Symantec					
Windows; Client Intrusion Detection System; Endpoint Protection Manager; Norton Security *Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft; The IDS can help identify patterns in network packets that may indicate an attack on the client; Symantec Endpoint Protection is a client-server solution that protects laptops,desktops, Windows and Mac computers, and servers in your network against malware;Norton Internet Security is an advanced security software for your PC.*					

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

Gain Information	2016-07-12	2.1	The GDI component in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to obtain sensitive kernel-address information via a crafted application, aka "Win32k Information Disclosure Vulnerability." **Reference: CVE-2016-3251**	http://technet.microsoft.com/en-us/security/bulletin/ms16-090	A-O-MIC-WINDO-250716/233
Novell, Phpmyadmin					
Leap, Opensuse, Phpmyadmin *LEAP, the Long range Energy Alternatives Planning System, is a widely-used software tool for energy policy analysis and climate change mitigation assessment developed at the Stockholm Environment Institute; The openSUSE project is a worldwide effort that promotes the use of Linux ; phpMyAdmin is a free and open source tool written in PHP intended to handle the administration of MySQL or MariaDB with the use of a web browser.*					
Gain Privileges	2016-07-12	7.2	The kernel-mode drivers in Microsoft Windows Server 2012 and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability." **Reference: CVE-2016-3250**	http://technet.microsoft.com/en-us/security/bulletin/ms16-090	A-O-NOV-LEAP-250716/234
Gain Privileges	2016-07-12	7.2	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3252, CVE-2016-3254, and CVE-2016-3286. **Reference: CVE-2016-3249**	http://technet.microsoft.com/en-us/security/bulletin/ms16-090	A-O-NOV-LEAP-250716/235
Denial of Service; Execute Code; Overflow;	2016-07-12	9.3	The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in	http://technet.microsoft.com/en-us/security/bull	A-O-NOV-LEAP-250716/236

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

Memory Corruption			Microsoft Internet Explorer 9 through 11, Microsoft Edge, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3259. **Reference: CVE-2016-3248**	etin/ms16-085	
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	7.6	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability." **Reference: CVE-2016-3246**	http://technet.microsoft.com/en-us/security/bulletin/ms16-085	A-O-NOV-LEAP,-250716/237
Bypass	2016-07-12	4.3	Microsoft Internet Explorer 9 through 11 allows remote attackers to trick users into making TCP connections to a restricted port via a crafted web site, aka "Internet Explorer Security Feature Bypass Vulnerability." **Reference: CVE-2016-3245**	http://technet.microsoft.com/en-us/security/bulletin/ms16-084	A-O-NOV-LEAP-250716/238
Bypass	2016-07-12	4.3	Microsoft Edge allows remote attackers to bypass the ASLR protection mechanism via a crafted web site, aka "Microsoft Edge Security Feature Bypass." **Reference: CVE-2016-3244**	http://technet.microsoft.com/en-us/security/bulletin/ms16-085	A-O-NOV-LEAP-250716/239
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	7.6	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability." **Reference: CVE-2016-3243**	http://technet.microsoft.com/en-us/security/bulletin/ms16-084	A-O-NOV-LEAP-250716/240
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	7.6	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka	http://technet.microsoft.com/en-us/security/bulletin/ms16-084	A-O-NOV-LEAP-250716/241

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

			"Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3240 and CVE-2016-3241. **Reference: CVE-2016-3242**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	7.6	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3240 and CVE-2016-3242. **Reference: CVE-2016-3241**	http://technet.microsoft.com/en-us/security/bulletin/ms16-084	A-O-NOV-OPENS-250716/242
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	7.6	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3241 and CVE-2016-3242. **Reference: CVE-2016-3240**	http://technet.microsoft.com/en-us/security/bulletin/ms16-084	A-O-NOV-OPENS-250716/243
Gain Privileges	2016-07-12	7.2	The Print Spooler service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via vectors involving filesystem write operations, aka "Windows Print Spooler Elevation of Privilege Vulnerability." **Reference: CVE-2016-3239**	http://technet.microsoft.com/en-us/security/bulletin/ms16-087	A-O-NOV-OPENS-250716/244
Redhat					
Ceph; Ceph Storage Mon; Ceph Storage Osd; Enterprise Linux Desktop; Enterprise Linux For Scientific Computing, Enterprise Linux Server; Enterprise Linux Workstation *In computing, Ceph, a free-software storage platform, implements object storage on a single distributed computer cluster, and provides interfaces for object-, block- and file-level storage. Ceph aims primarily for completely distributed operation without a single point of failure, scalable to the exabyte level, and freely available; Red Hat*					

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

Enterprise Linux (RHEL) is a Linux distribution developed by Red Hat and targeted toward the commercial market.					
Exec Code	2016-07-12	9.3	The Print Spooler service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows man-in-the-middle attackers to execute arbitrary code by providing a crafted print driver during printer installation, aka "Windows Print Spooler Remote Code Execution Vulnerability." **Reference: CVE-2016-3238**	http://technet.microsoft.com/en-us/security/bulletin/ms16-087	A-O-RED-CEPH-250716/245
Hardware					
Meinberg					
Ims-lantime M1000; Ims-lantime M3000; Ims-lantime M500; Lantime M100; M200; M300; M400; M600; M900; Lces; Ntp Server Firmware; Syncfire 1100 *The new LANTIME IMS series is a field-upgradable and extremely flexible system that covers your synchronization needs – today and in the future; NTP Client (Network Time Protocol) is the software client that allows your router to synchronize with an available time server; The Meinberg SyncFire 1100 NTP Time Server appliance offers the flexibility and reliability of the Meinberg.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-12	9.3	The Microsoft (1) Jscript 5.8 and 9 and (2) VBScript 5.7 and 5.8 engines, as used in Internet Explorer 9 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." **Reference: CVE-2016-3204**	http://technet.microsoft.com/en-us/security/bulletin/ms16-086	H-MEI-IMS-L-250716/246
Gain Privileges; Gain Information	2016-07-13	2.1	kinit in KDE Frameworks before 5.23.0 uses weak permissions (644) for /tmp/xauth-xxx-_y, which allows local users to obtain X11 cookies of other users and consequently capture keystrokes and possibly gain privileges by reading the file. **Reference: CVE-2016-3100**	https://www.kde.org/info/security/advisory-20160621-1.txt	H-MEI-IMS-L-250716/247
Denial of Service	2016-07-04	7.8	The MultipartStream class in	https://bugzilla.	H-MEI-IMS-L-

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

			Apache Commons Fileupload before 1.3.2, as used in Apache Tomcat 7.x before 7.0.70, 8.x before 8.0.36, 8.5.x before 8.5.3, and 9.x before 9.0.0.M7 and other products, allows remote attackers to cause a denial of service (CPU consumption) via a long boundary string. **Reference: CVE-2016-3092**	redhat.com/show_bug.cgi?id=1349468	250716/248
Hardware/ Operating System (H/OS)					
Ntt East					
Pr-400mi Firmware; Pr-400mi; Rt-400mi Firmware; Rv-440mi Firmware **NA**					
Bypass ; Gain Information	2016-07-02	5.5	IBM Security QRadar Incident Forensics 7.2.x before 7.2.7 allows remote attackers to bypass authentication, and obtain sensitive information or modify data, via unspecified vectors. **Reference: CVE-2016-2968**	http://www-01.ibm.com/support/docview.wss?uid=swg21985773	H-OS-NTT-PR-40-250716/249
Operating System (OS)					
Apple					
Airport Base Station Firmware *Apple periodically offers software updates (called firmware updates) that improve AirPort performance and functionality.*					
Gain Information	2016-07-02	5	The integration server in IBM Integration Bus 9 before 9.0.0.6 and 10 before 10.0.0.5 and WebSphere Message Broker 8 before 8.0.0.8 allows remote attackers to obtain sensitive Tomcat version information by sending a malformed POST request and then reading the Java stack trace. **Reference: CVE-2016-2961**	http://www-01.ibm.com/support/docview.wss?uid=swg21985017	O-APP-AIRPO-250716/250
Canonical, Linux					
Ubuntu Linux; Linux Kernel *Ubuntu is an open source software platform; The Linux kernel is a Unix-like computer operating system kernel.*					
Gain Privileges	2016-07-07	6	The API Discovery implementation in IBM WebSphere Application Server (WAS) 8.5.5.8 through 8.5.5.9 Liberty before Liberty Fix Pack 16.0.0.2 allows remote	http://www-01.ibm.com/support/docview.wss?uid=swg21984502	O-CAN-UBUNT-250716/251

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 gain privileges via an external reference in a Swagger document. **Reference: CVE-2016-2945**		
Gain Information	2016-07-07	5	IBM WebSphere Application Server (WAS) 8.5 through 8.5.5.9 Liberty before Liberty Fix Pack 16.0.0.2 does not include the HTTPOnly flag in a Set-Cookie header for an unspecified JAX-RS API cookie, which makes it easier for remote attackers to obtain potentially sensitive information via script access to this cookie. **Reference: CVE-2016-2923**	http://www-01.ibm.com/support/docview.wss?uid=swg21983700	O-CAN-UBUNT-250716/252
Cisco					
Epc3928 Firmware *EPC3928 firmware is a wireless Residential Voice Gateway.*					
Gain Information	2016-07-03	2.1	IBM Spectrum Protect (formerly Tivoli Storage Manager) 5.5 through 6.3 before 6.3.2.6, 6.4 before 6.4.3.3, and 7.1 before 7.1.6 allows local users to obtain sensitive retrieved data from arbitrary accounts in opportunistic circumstances by leveraging previous use of a symlink during archive and retrieve actions. **Reference: CVE-2016-2894**	http://www-01.ibm.com/support/docview.wss?uid=swg21985579	O-CIS-EPC39-250716/253
Cross Site Request Forgery	2016-07-07	6.8	Cross-site request forgery (CSRF) vulnerability in the Report Builder and Data Collection Component (DCC) in IBM Jazz Reporting Service (JRS) 5.x before 5.0.2 ifix016, 6.0 and 6.0.1 before 6.0.1 ifix005, and 6.0.2 before ifix002 allows remote authenticated users to hijack the authentication of arbitrary users. **Reference: CVE-2016-2889**	http://www-01.ibm.com/support/docview.wss?uid=swg21983147	O-CIS-EPC39-250716/254
Cross Site Scripting	2016-07-07	4.3	Cross-site scripting (XSS) vulnerability in the Report Builder and Data Collection	http://www-01.ibm.com/support/docview.ws	O-CIS-EPC39-250716/255

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

			Component (DCC) in IBM Jazz Reporting Service (JRS) 5.x before 5.0.2 ifix016 and 6.x before 6.0.1 ifix005 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL, a different vulnerability than CVE-2016-0313 and CVE-2016-0350. **Reference: CVE-2016-2888**	s?uid=swg21983147	
IOS *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc.*					
Cross Site Scripting	2016-07-02	3.5	Cross-site scripting (XSS) vulnerability in IBM TRIRIGA Application Platform 3.3 before 3.3.2.6, 3.4 before 3.4.2.4, and 3.5 before 3.5.0.2 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-2883**	http://www-01.ibm.com/support/docview.wss?uid=swg21983347	O-CIS-IOS-250716/256
Ios Xr *IOS XR is a train of Cisco Systems' widely deployed Internetworking Operating System (IOS), used on their high-end carrier-grade routers such as the CRS series, 12000 series, and ASR9000 series.*					
Gain Information	2016-07-02	4	IBM TRIRIGA Application Platform 3.3 before 3.3.2.6, 3.4 before 3.4.2.4, and 3.5 before 3.5.0.2 allows remote authenticated users to obtain sensitive information by reading HTTP responses. **Reference: CVE-2016-2882**	http://www-01.ibm.com/support/docview.wss?uid=swg21983343	O-CIS-IOS X-250716/257
Ios Xr *IOS XR is a train of Cisco Systems' widely deployed Internetworking Operating System (IOS), used on their high-end carrier-grade routers such as the CRS series, 12000 series, and ASR9000 series.*					
Directory Traversal	2016-07-02	5	Directory traversal vulnerability in IBM Security QRadar SIEM 7.2.x before 7.2.7 and QRadar Incident Forensics 7.2.x before 7.2.7 allows remote attackers to read arbitrary files via a crafted URL. **Reference: CVE-2016-2872**	http://www-01.ibm.com/support/docview.wss?uid=swg21985775	O-CIS-IOS X-250716/258
IOS; Ios Xe *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc; Cisco IOS XE software provides a modular structure that significantly enhances software quality and performance by separating the data plane and control plan.*					

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

Denial of Service; Overflow	2016-07-02	5	Buffer overflow in the CLI on IBM WebSphere DataPower XC10 appliances 2.1 and 2.5 allows remote authenticated users to cause a denial of service via unspecified vectors. **Reference: CVE-2016-2870**	http://www-01.ibm.com/support/docview.wss?uid=swg21983035	O-CIS-IOS; -250716/259
Rv110w Firmware; Rv130w Firmware; Rv215w Firmware *Cisco Small Business RV Series Routers provides small businesses (SMB) with highly secure VPN access, security with built-in firewalls, and simple installation.*					
NA	2016-07-02	4	IBM Security QRadar SIEM 7.2.x before 7.2.7 allows remote authenticated administrators to read arbitrary files via XML data containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. **Reference: CVE-2016-2868**	http://www-01.ibm.com/support/docview.wss?uid=swg21985774	O-CIS-RV110-250716/260
Debian, Linux					
Debian Linux, Linux Kernel *Debian is an operating system and a distribution of Free Software; The Linux kernel is a Unix-like computer operating system kernel.*					
NA	2016-07-02	6.9	IBM InfoSphere Streams before 4.0.1.2 and IBM Streams before 4.1.1.1 do not properly implement the runAsUser feature, which allows local users to obtain root group privileges via unspecified vectors. **Reference: CVE-2016-2867**	http://www-01.ibm.com/support/docview.wss?uid=swg21983444	O-DEB-DEBIA-250716/261
Google					
Android *Android is an OS created by Google for use on mobile devices, such as smartphones and tablets*					
Cross Site Scripting; Cross Site Request Forgery	2016-07-03	6	Cross-site request forgery (CSRF) vulnerability in IBM WebSphere Commerce 7.0 Feature Pack 8, 8.0.0.x before 8.0.0.10, and 8.0.1.x before 8.0.1.2 allows remote authenticated users to hijack the authentication of arbitrary users for requests that insert XSS sequences. **Reference: CVE-2016-2863**	http://www-01.ibm.com/support/docview.wss?uid=swg21983626	O-GOO-ANDRO-250716/262
Cross Site Scripting	2016-07-03	4.3	Cross-site scripting (XSS) vulnerability in IBM WebSphere	http://www-01.ibm.com/sup	O-GOO-ANDRO-

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

			Commerce 6.0 through 6.0.0.11, 7.0 before 7.0.0.9 cumulative iFix 3, and 8.0 before 8.0.0.5 allows remote attackers to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-2862**	port/docview.wss?uid=swg21983625	250716/263
Gain Information	2016-07-02	4.3	IBM WebSphere eXtreme Scale 7.1.0 before 7.1.0.3, 7.1.1 before 7.1.1.1, 8.5 before 8.5.0.3, and 8.6 before 8.6.0.8 does not properly encrypt data, which makes it easier for remote attackers to obtain sensitive information by sniffing the network. **Reference: CVE-2016-2861**	http://www-01.ibm.com/support/docview.wss?uid=swg21983036	O-GOO-ANDRO-250716/264
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-10	9.3	media/libmediaplayerservice/nuplayer/GenericSource.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 does not validate certain track data, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28799341. **Reference: CVE-2016-2508**	https://android.googlesource.com/platform/frameworks/av/+/f81038006b4c59a5a148dcad887371206033c28f	O-GOO-ANDRO-250716/265
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-10	9.3	Integer overflow in codecs/on2/h264dec/source/h264bsd_storage.c in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28532266. **Reference: CVE-2016-2507**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/266
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-10	10	DRMExtractor.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 does not validate a certain offset value, which allows remote	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/267

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

			attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28175045. **Reference: CVE-2016-2506**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-10	9.3	mpeg2ts/ATSParser.cpp in libstagefright in mediaserver in Android 6.x before 2016-07-01 does not validate a certain section length, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28333006. **Reference: CVE-2016-2505**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/268
Gain Privileges	2016-07-10	9.3	The Qualcomm GPU driver in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28084795 and Qualcomm internal bug CR1006067. **Reference: CVE-2016-2503**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/269
Gain Privileges	2016-07-10	9.3	drivers/usb/gadget/f_serial.c in the Qualcomm USB driver in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a large size in a GSER_IOCTL ioctl call, aka Android internal bug 27657963 and Qualcomm internal bug CR997044. **Reference: CVE-2016-2502**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/270
Gain Privileges	2016-07-10	9.3	The Qualcomm camera driver in Android before 2016-07-05 on Nexus 5X, 6, 6P, and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 27890772 and Qualcomm internal bug CR1001092. **Reference: CVE-2016-2501**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/271
Cross Site Scripting	2016-07-12	3.5	Cross-site scripting (XSS) vulnerability in the management interface in Palo Alto Networks PAN-OS 7.x	https://securityadvisories.paloaltonetworks.com/Home/Detail/4	O-GOO-ANDRO-250716/272

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

			before 7.0.8 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-2219**	2	
NA	2016-07-11	3.3	The management console in Symantec Workspace Streaming (SWS) 7.5.x before 7.5 SP1 HF9 and 7.6.0 before 7.6 HF5 and Symantec Workspace Virtualization (SWV) 7.5.x before 7.5 SP1 HF9 and 7.6.0 before 7.6 HF5 allows remote authenticated users to read arbitrary files by modifying the file-download configuration file. **Reference: CVE-2016-2206**	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160707_00	O-GOO-ANDRO-250716/273
Directory Traversal	2016-07-11	6.1	Directory traversal vulnerability in the file-download configuration file in the management console in Symantec Workspace Streaming (SWS) 7.5.x before 7.5 SP1 HF9 and 7.6.0 before 7.6 HF5 and Symantec Workspace Virtualization (SWV) 7.5.x before 7.5 SP1 HF9 and 7.6.0 before 7.6 HF5 allows remote authenticated users to read unspecified application files via unknown vectors. **Reference: CVE-2016-2205**	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160707_00	O-GOO-ANDRO-250716/274
Bypass	2016-07-07	6.8	libcli/smb/smbXcli_base.c in Samba 4.x before 4.2.14, 4.3.x before 4.3.11, and 4.4.x before 4.4.5 allows man-in-the-middle attackers to bypass a client-signing protection mechanism, and consequently spoof SMB2 and SMB3 servers, via the (1) SMB2_SESSION_FLAG_IS_GUEST or (2) SMB2_SESSION_FLAG_IS_NULL flag. **Reference: CVE-2016-2119**	https://www.samba.org/samba/security/CVE-2016-2119.html	O-GOO-ANDRO-250716/275
Cross Site Request Forgery	2016-07-02	6.8	Cross-site request forgery (CSRF) vulnerability in VMware vRealize Log Insight 2.x and 3.x before 3.3.2 allows remote attackers to hijack the	http://www.vmware.com/security/advisories/VMSA-2016-0008.html	O-GOO-ANDRO-250716/276

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

			authentication of unspecified victims via unknown vectors. **Reference: CVE-2016-2082**		
Cross Site Scripting	2016-07-02	4.3	Cross-site scripting (XSS) vulnerability in VMware vRealize Log Insight 2.x and 3.x before 3.3.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-2081**	http://www.vmware.com/security/advisories/VMSA-2016-0008.html	O-GOO-ANDRO-250716/277
Gain Information	2016-07-02	4.3	VMware NSX Edge 6.1 before 6.1.7 and 6.2 before 6.2.3 and vCNS Edge 5.5 before 5.5.4.3, when the SSL-VPN feature is configured, allow remote attackers to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-2079**	http://www.vmware.com/security/advisories/VMSA-2016-0007.html	O-GOO-ANDRO-250716/278
Execute Code; Overflow	2016-07-03	7.5	Buffer overflow in lib/flow.c in ovs-vswitchd in Open vSwitch 2.2.x and 2.3.x before 2.3.3 and 2.4.x before 2.4.1 allows remote attackers to execute arbitrary code via crafted MPLS packets, as demonstrated by a long string in an ovs-appctl command. **Reference: CVE-2016-2074**	https://bugzilla.redhat.com/show_bug.cgi?id=1318553	O-GOO-ANDRO-250716/279
Denial of Service; Overflow; Gain Privileges	2016-07-10	9.3	The MSM QDSP6 audio driver (aka sound driver) for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to gain privileges or cause a denial of service (integer overflow, and buffer overflow or buffer over-read) via a crafted application that performs a (1) AUDIO_EFFECTS_WRITE or (2) AUDIO_EFFECTS_READ operation, aka Qualcomm internal bug CR1006609. **Reference: CVE-2016-2068**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/280
Gain Privileges	2016-07-10	9.3	drivers/gpu/msm/kgsl.c in the MSM graphics driver (aka GPU driver) for the Linux kernel 3.x,	https://source.codeaurora.org/quic/la//kernel/	O-GOO-ANDRO-250716/281

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

			as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, mishandles the KGSL_MEMFLAGS_GPUREADONLY flag, which allows attackers to gain privileges by leveraging accidental read-write mappings, aka Qualcomm internal bug CR988993. **Reference: CVE-2016-2067**	msm-3.18/commit/?id=410cfa95f0a1cf58819cbfbd896f9aa45b004ac0	
Denial of Service	2016-07-03	6.8	Multiple unspecified vulnerabilities in Google Chrome before 51.0.2704.103 allow attackers to cause a denial of service or possibly have other impact via unknown vectors. **Reference: CVE-2016-1704**	http://googlechromereleases.blogspot.com/2016/06/stable-channel-update_16.html	O-GOO-ANDRO-250716/282
Execute Code; Overflow	2016-07-02	10	Multiple stack-based buffer overflows in COM objects in Micro Focus Rumba 9.4.x before 9.4 HF 13960 allow remote attackers to execute arbitrary code via (1) the NetworkName property value to ObjectXSNAConfig.ObjectXSNAConfig in iconfig.dll, (2) the CPName property value to ObjectXSNAConfig.ObjectXSNAConfig in iconfig.dll, (3) the PrinterName property value to ProfileEditor.PrintPasteControl in ProfEdit.dll, (4) the Data argument to the WriteRecords function in FTXBIFFLib.AS400FtxBIFF in FtxBIFF.dll, (5) the Serialized property value to NMSECCOMPARAMSLib.SSL3 in NMSecComParams.dll, (6) the UserName property value to NMSECCOMPARAMSLib.FirewallProxy in NMSecComParams.dll, (7) the LUName property value to ProfileEditor.MFSNAControl in ProfEdit.dll, (8) the newVal argument to the Load function in FTPSFTPLib.SFtpSession in FTPSFtp.dll, or (9) a long Host	http://community.microfocus.com/microfocus/mainframe_solutions/rumba/w/knowledge_base/28601.rumba-9-4-stack-buffer-overflow-vulnerabilities.aspx	O-GOO-ANDRO-250716/283

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

			field in the FTP Client. **Reference: CVE-2016-1606**		
Denial of Service	2016-07-06	4.3	The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows. **Reference: CVE-2016-1546**	http://httpd.apache.org/security/vulnerabilities_24.html	O-GOO-ANDRO-250716/284
NA	2016-07-15	6	Cisco WebEx Meetings Server 2.6 allows remote authenticated users to conduct command-injection attacks via vectors related to an upload's file type, aka Bug ID CSCuy92715. **Reference: CVE-2016-1450**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160714-wms4	O-GOO-ANDRO-250716/285
Cross Site Scripting	2016-07-15	4.3	Cross-site scripting (XSS) vulnerability in Cisco WebEx Meetings Server 2.6 allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka Bug ID CSCuy92711. **Reference: CVE-2016-1449**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160714-wms3	O-GOO-ANDRO-250716/286
Cross Site Scripting	2016-07-15	4.3	Cross-site scripting (XSS) vulnerability in the administrator interface in Cisco WebEx Meetings Server 2.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka Bug ID CSCuy83194. **Reference: CVE-2016-1447**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160714-wms1	O-GOO-ANDRO-250716/287
Execute Code; SQL Injection	2016-07-15	6.5	SQL injection vulnerability in Cisco WebEx Meetings Server 2.6 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors, aka Bug ID CSCuy83200. **Reference: CVE-2016-1446**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160714-wms	O-GOO-ANDRO-250716/288
Bypass	2016-07-11	4.3	Cisco Adaptive Security Appliance (ASA) Software 8.2 through 9.4.3.3 allows remote attackers to bypass intended ICMP Echo Reply ACLs via	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-GOO-ANDRO-250716/289

			vectors related to subtypes. **Reference: CVE-2016-1445**	20160711-asa	
Bypass	2016-07-07	5.8	The Mobile and Remote Access (MRA) component in Cisco TelePresence Video Communication Server (VCS) X8.1 through X8.7 and Expressway X8.1 through X8.6 mishandles certificates, which allows remote attackers to bypass authentication via an arbitrary trusted certificate, aka Bug ID CSCuz64601. **Reference: CVE-2016-1444**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160706-vcs	O-GOO-ANDRO-250716/290
Bypass; Gain Information	2016-07-07	6.8	The virtual network stack on Cisco AMP Threat Grid Appliance devices before 2.1.1 allows remote attackers to bypass a sandbox protection mechanism, and consequently obtain sensitive interprocess information or modify interprocess data, via a crafted malware sample. **Reference: CVE-2016-1443**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160706-tg	O-GOO-ANDRO-250716/291
Execute Code	2016-07-07	9	The administrative web interface in Cisco Prime Infrastructure (PI) before 3.1.1 allows remote authenticated users to execute arbitrary commands via crafted field values, aka Bug ID CSCuy96280. **Reference: CVE-2016-1442**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160706-pi	O-GOO-ANDRO-250716/292
Bypass	2016-07-02	6.4	Cisco Cloud Network Automation Provisioner (CNAP) 1.0(0) in Cisco Configuration Assistant (CCA) allows remote attackers to bypass intended filesystem and administrative-endpoint restrictions via GET API calls, aka Bug ID CSCuy77145. **Reference: CVE-2016-1441**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160630-cca	O-GOO-ANDRO-250716/293
Denial of Service	2016-07-02	5	The proxy process on Cisco Web Security Appliance (WSA) devices through 9.1.0-070 allows remote attackers to cause a denial of service (CPU consumption) by establishing an FTP session and then	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160627-wsa	O-GOO-ANDRO-250716/294

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

			improperly terminating the control connection after a file transfer, aka Bug ID CSCuy43468. **Reference: CVE-2016-1440**		
Denial of Service; Overflow	2016-07-03	6.1	Cisco IOS 15.0(2)SG5, 15.1(2)SG3, 15.2(1)E, 15.3(3)S, and 15.4(1.13)S allows remote attackers to cause a denial of service (device crash) via a crafted LLDP packet, aka Bug ID CSCun66735. **Reference: CVE-2016-1425**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160616-ios1	O-GOO-ANDRO-250716/295
NA	2016-07-02	10	Cisco Prime Collaboration Provisioning 10.6 SP2 (aka 10.6.0.10602) mishandles LDAP authentication, which allows remote attackers to obtain administrator privileges via a crafted login attempt, aka Bug ID CSCuv37513. **Reference: CVE-2016-1416**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160629-cpcpauthbypass	O-GOO-ANDRO-250716/296
Execute Code	2016-07-02	6.5	Cisco Prime Infrastructure 1.2 through 3.1 and Evolved Programmable Network Manager (EPNM) 1.2 and 2.0 allow remote authenticated users to execute arbitrary commands or upload files via a crafted HTTP request, aka Bug ID CSCuz01488. **Reference: CVE-2016-1408**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160629-pi-epnm	O-GOO-ANDRO-250716/297
Denial of Service; Overflow	2016-07-03	6.8	Buffer overflow in the web-based management interface on Cisco RV110W devices with firmware through 1.2.1.4, RV130W devices with firmware through 1.0.2.7, and RV215W devices with firmware through 1.3.0.7 allows remote authenticated users to cause a denial of service (device reload) via a crafted HTTP request, aka Bug ID CSCux86669. **Reference: CVE-2016-1398**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-rv3	O-GOO-ANDRO-250716/298
NA	2016-07-02	7.5	Cisco Firepower System Software 6.0.0 through 6.1.0 has a hardcoded account, which allows remote attackers to obtain CLI access by leveraging	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-GOO-ANDRO-250716/299

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

			knowledge of the password, aka Bug ID CSCuz56238. **Reference: CVE-2016-1394**	20160629-fp	
Gain Information	2016-07-03	4.3	Cisco EPC3928 devices allow remote attackers to obtain sensitive configuration and credential information by making requests during the early part of the boot process, related to a "Boot Information Disclosure" issue, aka Bug ID CSCux17178. **Reference: CVE-2016-1337**	http://www.securityfocus.com/archive/1/archive/1/538627/100/0/threaded	O-GOO-ANDRO-250716/300
Denial of Service	2016-07-03	7.8	goform/Docsis_system on Cisco EPC3928 devices allows remote attackers to cause a denial of service (device crash) via a long LanguageSelect parameter, related to a "Gateway HTTP Corruption Denial of Service" issue, aka Bug ID CSCuy28100. **Reference: CVE-2016-1336**	http://secorda.com/multiple-security-vulnerabilities-affecting-cisco-epc3928/	O-GOO-ANDRO-250716/301
Denial of Service	2016-07-03	7.8	goform/WClientMACList on Cisco EPC3928 devices allows remote attackers to cause a denial of service (device crash) via a long h_sortWireless parameter, related to a "Gateway Client List Denial of Service" issue, aka Bug ID CSCux24948. **Reference: CVE-2016-1328**	http://secorda.com/multiple-security-vulnerabilities-affecting-cisco-epc3928/	O-GOO-ANDRO-250716/302
Execute Code; Overflow; Gain Information	2016-07-02	10	The API in Cisco Prime Infrastructure 1.2 through 3.0 and Evolved Programmable Network Manager (EPNM) 1.2 allows remote attackers to execute arbitrary code or obtain sensitive management information via a crafted HTTP request, as demonstrated by discovering managed-device credentials, aka Bug ID CSCuy10231. **Reference: CVE-2016-1289**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160629-piauthbypass	O-GOO-ANDRO-250716/303
Cross Site Request Forgery	2016-07-03	6.8	Cross-site request forgery (CSRF) vulnerability on NTT EAST Hikari Denwa routers with firmware PR-400MI, RT-400MI, and RV-440MI	http://www.ntt-west.co.jp/kiki/support/flets/hgw4_mi/160627.html	O-GOO-ANDRO-250716/304

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

			07.00.1006 and earlier and NTT WEST Hikari Denwa routers with firmware PR-400MI, RT-400MI, and RV-440MI 07.00.1005 and earlier allows remote attackers to hijack the authentication of arbitrary users. **Reference: CVE-2016-1228**		
Execute Code	2016-07-03	6.5	NTT EAST Hikari Denwa routers with firmware PR-400MI, RT-400MI, and RV-440MI 07.00.1006 and earlier and NTT WEST Hikari Denwa routers with firmware PR-400MI, RT-400MI, and RV-440MI 07.00.1005 and earlier allow remote authenticated users to execute arbitrary OS commands via unspecified vectors. **Reference: CVE-2016-1227**	http://www.ntt-west.co.jp/kiki/support/flets/hgw4_mi/160627.html	O-GOO-ANDRO-250716/305
Denial of Service; Cross Site Scripting	2016-07-04	6.4	ActionServlet.java in Apache Struts 1 1.x through 1.3.10 does not properly restrict the Validator configuration, which allows remote attackers to conduct cross-site scripting (XSS) attacks or cause a denial of service via crafted input, a related issue to CVE-2015-0899. **Reference: CVE-2016-1182**	https://github.com/kawasima/struts1-forever/commit/eda3a79907ed8fcb0387a0496d0cb14332f250e8	O-GOO-ANDRO-250716/306
Denial of Service; Execute Code	2016-07-04	6.8	ActionServlet.java in Apache Struts 1 1.x through 1.3.10 mishandles multithreaded access to an ActionForm instance, which allows remote attackers to execute arbitrary code or cause a denial of service (unexpected memory access) via a multipart request, a related issue to CVE-2015-0899. **Reference: CVE-2016-1181**	https://github.com/kawasima/struts1-forever/commit/eda3a79907ed8fcb0387a0496d0cb14332f250e8	O-GOO-ANDRO-250716/307
NA	2016-07-06	6.5	The web-restore interface in Avamar Data Store (ADS) and Avamar Virtual Edition (AVE) in EMC Avamar through 7.1.2 and 7.2.x through 7.2.1 allows remote authenticated users to	http://seclists.org/bugtraq/2016/Jul/33	O-GOO-ANDRO-250716/308

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

			read or delete directories via a Linux backup-restore operation. **Reference: CVE-2016-0906**		
Gain Information	2016-07-04	3.5	EMC RSA Archer GRC 5.5.x before 5.5.3.4 allows remote authenticated users to read the web.config.bak file, and obtain sensitive credential information, by modifying the IIS configuration to set a Content-Type header for .bak files. **Reference: CVE-2016-0899**	http://seclists.org/bugtraq/2016/Jun/54	O-GOO-ANDRO-250716/309
Http R.Spl.	2016-07-02	4.3	CRLF injection vulnerability in IBM WebSphere eXtreme Scale 7.1.0 before 7.1.0.3, 7.1.1 before 7.1.1.1, 8.5 before 8.5.0.3, and 8.6 before 8.6.0.8 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via a crafted URL. **Reference: CVE-2016-0400**	http://www-01.ibm.com/support/docview.wss?uid=swg21983036	O-GOO-ANDRO-250716/310
Cross Site Scripting	2016-07-02	3.5	Cross-site scripting (XSS) vulnerability in IBM Maximo Asset Management 7.1 through 7.1.1.13, 7.5 before 7.5.0.9 IFIX007, and 7.6 before 7.6.0.5 FP005 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. CVE-2016-0399	http://www-01.ibm.com/support/docview.wss?uid=swg21984134	O-GOO-ANDRO-250716/311
NA	2016-07-02	4.3	IBM Cognos Analytics (CA) 11.0 before 11.0.2 allows remote attackers to conduct content-spoofing attacks via a crafted URL. **Reference: CVE-2016-0398**	http://www-01.ibm.com/support/docview.wss?uid=swg21977070	O-GOO-ANDRO-250716/312
NA	2016-07-02	7.5	The IBM Watson Developer Cloud services on Bluemix platforms do not properly generate random numbers for service-instance credentials, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.	http://www-01.ibm.com/support/docview.wss?uid=swg21982615	O-GOO-ANDRO-250716/313

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-2016-0391		
Gain Information	2016-07-07	5	Admin Center in IBM WebSphere Application Server (WAS) 8.5.5.2 through 8.5.5.9 Liberty before Liberty Fix Pack 16.0.0.2 allows remote attackers to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-0389**	http://www-01.ibm.com/support/docview.wss?uid=swg21982012	O-GOO-ANDRO-250716/314
Cross Site Scripting	2016-07-02	3.5	Cross-site scripting (XSS) vulnerability in IBM TRIRIGA Application Platform 3.3 before 3.3.2.6, 3.4 before 3.4.2.4, and 3.5 before 3.5.0.2 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-0387**	http://www-01.ibm.com/support/docview.wss?uid=swg21981740	O-GOO-ANDRO-250716/315
Cross Site Request Forgery	2016-07-02	6	Cross-site request forgery (CSRF) vulnerability in IBM TRIRIGA Application Platform 3.3 before 3.3.2.6, 3.4 before 3.4.2.4, and 3.5 before 3.5.0.2 allows remote authenticated users to hijack the authentication of administrators for requests that delete employees. **Reference: CVE-2016-0386**	http://www-01.ibm.com/support/docview.wss?uid=swg1IV83657	O-GOO-ANDRO-250716/316
Http R.Spl.	2016-07-03	4.3	CRLF injection vulnerability in IBM WebSphere Application Server (WAS) 7.0 before 7.0.0.43, 8.0 before 8.0.0.13, 8.5 Full before 8.5.5.10, and 8.5 Liberty before Liberty Fix Pack 16.0.0.2 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via a crafted URL. **Reference: CVE-2016-0359**	http://www-01.ibm.com/support/docview.wss?uid=swg21982526	O-GOO-ANDRO-250716/317
Cross Site Scripting	2016-07-07	3.5	Cross-site scripting (XSS) vulnerability in the Report Builder and Data Collection Component (DCC) in IBM Jazz Reporting Service (JRS) 5.x	http://www-01.ibm.com/support/docview.wss?uid=swg21983147	O-GOO-ANDRO-250716/318

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

			before 5.0.2 ifix016 and 6.x before 6.0.1 ifix005 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL, a different vulnerability than CVE-2016-2888 and CVE-2016-0313. **Reference: CVE-2016-0350**		
Cross Site Scripting	2016-07-03	3.5	Cross-site scripting (XSS) vulnerability in IBM Cognos Business Intelligence 10.2 before IF20, 10.2.1 before IF17, 10.2.1.1 before IF16, 10.2.2 before IF12, and 10.1.1 before IF19 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-0346**	http://www-01.ibm.com/support/docview.wss?uid=swg21984323	O-GOO-ANDRO-250716/319
NA	2016-07-07	6.5	The Report Builder and Data Collection Component (DCC) in IBM Jazz Reporting Service (JRS) 5.x before 5.0.2 ifix016 and 6.x before 6.0.1 ifix005 maintain session ID validity after a logout action, which allows remote authenticated users to hijack sessions by leveraging an unattended workstation. **Reference: CVE-2016-0315**	http://www-01.ibm.com/support/docview.wss?uid=swg21983147	O-GOO-ANDRO-250716/320
NA	2016-07-07	4	The Report Builder and Data Collection Component (DCC) in IBM Jazz Reporting Service (JRS) 5.x before 5.0.2 ifix016 and 6.x before 6.0.1 ifix005 allow remote authenticated users to conduct clickjacking attacks via unspecified vectors. **Reference: CVE-2016-0314**	http://www-01.ibm.com/support/docview.wss?uid=swg21983147	O-GOO-ANDRO-250716/321
Cross Site Scripting	2016-07-07	3.5	Cross-site scripting (XSS) vulnerability in the Report Builder and Data Collection Component (DCC) in IBM Jazz Reporting Service (JRS) 5.x before 5.0.2 ifix016 and 6.x before 6.0.1 ifix005 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL, a	http://www-01.ibm.com/support/docview.wss?uid=swg21983147	O-GOO-ANDRO-250716/322

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

			different vulnerability than CVE-2016-2888 and CVE-2016-0350. **Reference: CVE-2016-0313**		
NA	2016-07-07	2.1	IBM i Access 7.1 on Windows allows local users to discover registry passwords via unspecified vectors. **Reference: CVE-2016-0287**	http://www-01.ibm.com/support/docview.wss?uid=nas8N1021418	O-GOO-ANDRO-250716/323
NA	2016-07-07	7.2	The agents in IBM UrbanCode Deploy 6.x before 6.0.1.14, 6.1.x before 6.1.3.3, and 6.2.x before 6.2.1.1 do not verify a server's identity in a JMS session or an HTTP session, which allows local users to obtain root access to arbitrary agents via unspecified vectors. **Reference: CVE-2016-0271**	http://www-01.ibm.com/support/docview.wss?uid=swg2C1000150	O-GOO-ANDRO-250716/324
Gain Information	2016-07-07	1.9	IBM Control Center 6.x before 6.0.0.1 iFix06 and Sterling Control Center 5.4.x before 5.4.2.1 iFix09 allow local users to decrypt the master key via unspecified vectors. **Reference: CVE-2016-0252**	http://www-01.ibm.com/support/docview.wss?uid=swg21985641	O-GOO-ANDRO-250716/325
NA	2016-07-07	7.2	IBM Power Hardware Management Console (HMC) 7.3 through 7.3.0 SP7, 7.9 through 7.9.0 SP3, 8.1 through 8.1.0 SP3, 8.2 through 8.2.0 SP2, 8.3 through 8.3.0 SP2, 8.4 through 8.4.0 SP1, and 8.5.0 allows physically proximate attackers to obtain root access via unspecified vectors. **Reference: CVE-2016-0230**	https://delivery04.dhe.ibm.com/sar/CMA/HMA/06a2q/1/MH01640.readme.html	O-GOO-ANDRO-250716/326
Cross Site Scripting	2016-07-03	3.5	Cross-site scripting (XSS) vulnerability in IBM Cognos TM1, as used in IBM Cognos Business Intelligence 10.2 before IF20, 10.2.1 before IF17, 10.2.1.1 before IF16, 10.2.2 before IF12, and 10.1.1 before IF19, allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-0221**	http://www-01.ibm.com/support/docview.wss?uid=swg21984323	O-GOO-ANDRO-250716/327
Denial of Service;	2016-07-10	4.3	app/aboot/aboot.c in the	http://source.an	O-GOO-

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

Overflow			Qualcomm bootloader in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allows attackers to cause a denial of service (OS outage or buffer over-read) via a crafted application, aka Android internal bug 28822690 and Qualcomm internal bug CR822275. **Reference: CVE-2015-8893**	droid.com/security/bulletin/2016-07-01.html	ANDRO-250716/328
Bypass	2016-07-10	9.3	platform/msm_shared/boot_verifier.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to bypass intended access restrictions via a digest with trailing data, aka Android internal bug 28822807 and Qualcomm internal bug CR902998. **Reference: CVE-2015-8892**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/329
Overflow; Bypass	2016-07-10	9.3	Multiple integer overflows in app/aboot/aboot.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allow attackers to bypass intended access restrictions via a crafted image, aka Android internal bug 28842418 and Qualcomm internal bug CR813930. **Reference: CVE-2015-8891**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/330
Bypass	2016-07-10	9.3	platform/msm_shared/partition_parser.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate certain GUID Partition Table (GPT) data, which allows attackers to bypass intended access restrictions via a crafted MultiMediaCard (MMC), aka Android internal bug 28822878 and Qualcomm internal bug CR823461. **Reference: CVE-2015-8890**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/331
NA	2016-07-10	9.3	The aboot implementation in the Qualcomm components in	http://source.android.com/secur	O-GOO-ANDRO-

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

			Android before 2016-07-05 on Nexus 6P devices omits the recovery PIN feature, which has unspecified impact and attack vectors, aka Android internal bug 28822677 and Qualcomm internal bug CR804067. **Reference: CVE-2015-8889**	ity/bulletin/2016-07-01.html	250716/332
Overflow; Bypass	2016-07-10	9.3	Integer overflow in app/aboot/aboot.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices allows attackers to bypass intended access restrictions via a crafted block count and block size of a sparse header, aka Android internal bug 28822465 and Qualcomm internal bug CR813933. **Reference: CVE-2015-8888**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/333
Denial of Service; Overflow	2016-07-13	4.3	The DecodeImage function in coders/gif.c in GraphicsMagick 1.3.18 allows remote attackers to cause a denial of service (uninitialized memory access) via a crafted GIF file. **Reference: CVE-2015-8808**	http://www.openwall.com/lists/oss-security/2016/02/06/3	O-GOO-ANDRO-250716/334
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-07-02	10	Apple AirPort Base Station Firmware before 7.6.7 and 7.7.x before 7.7.7 misparses DNS data, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference: CVE-2015-7029**	https://support.apple.com/HT206849	O-GOO-ANDRO-250716/335
Cross Site Scripting	2016-07-02	4.3	Cross-site scripting (XSS) vulnerability in the vSphere Web Client in VMware vCenter Server 5.0 before U3g, 5.1 before U3d, and 5.5 before U2d allows remote attackers to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2015-6931**	http://www.vmware.com/security/advisories/VMSA-2016-0009.html	O-GOO-ANDRO-250716/336
Cross Site Scripting	2016-07-03	4.3	Cross-site scripting (XSS) vulnerability in File Station in QNAP QTS before 4.2.0 allows remote attackers to inject	https://www.qnap.com/i/en/support/con_show.php?cid=93	O-GOO-ANDRO-250716/337

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

			arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2015-5664**		
Denial of Service; Overflow	2016-07-12	4.3	Pivotal Spring Framework before 3.2.14 and 4.x before 4.1.7 do not properly process inline DTD declarations when DTD is not entirely disabled, which allows remote attackers to cause a denial of service (memory consumption and out-of-memory errors) via a crafted XML file. **Reference: CVE-2015-3192**	https://jira.spring.io/browse/SPR-13136	O-GOO-ANDRO-250716/338
Bypass	2016-07-04	5	The MultiPageValidator implementation in Apache Struts 1 1.1 through 1.3.10 allows remote attackers to bypass intended access restrictions via a modified page parameter. **Reference: CVE-2015-0899**	https://en.osdn.jp/projects/terasoluna/wiki/StrutsPatch2-EN	O-GOO-ANDRO-250716/339
Gain Privileges	2016-07-10	9.3	arch/arm64/include/asm/pgtable.h in the Linux kernel before 3.15-rc5-next-20140519, as used in Android before 2016-07-05 on Nexus 5X and 6P devices, mishandles execute-only pages, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28557020. **Reference: CVE-2014-9803**	https://github.com/torvalds/linux/commit/5a0fdfada3a2aa50d7b947a2e958bf00cbe0d830	O-GOO-ANDRO-250716/340
Overflow ; Gain Privileges	2016-07-10	9.3	Multiple integer overflows in lib/libfdt/fdt.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allow attackers to gain privileges via a crafted application, aka Android internal bug 28821965 and Qualcomm internal bug CR705108. **Reference: CVE-2014-9802**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/341
Overflow ; Gain Privileges	2016-07-10	9.3	Multiple integer overflows in lib/libfdt/fdt_rw.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices allow attackers to gain privileges via a crafted	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/342

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

			application, aka Android internal bug 28822060 and Qualcomm internal bug CR705078. **Reference: CVE-2014-9801**		
Google; Linux					
Android; Linux Kernel *Android is an OS created by Google for use on mobile devices, such as smartphones and tablets; The Linux kernel is a Unix-like computer operating system kernel.*					
Overflow ; Gain Privileges	2016-07-10	9.3	Integer overflow in lib/heap/heap.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28822150 and Qualcomm internal bug CR692478. **Reference: CVE-2014-9800**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/343
Overflow ; Gain Privileges	2016-07-10	9.3	The makefile in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices omits the -fno-strict-overflow option to gcc, which might allow attackers to gain privileges via a crafted application that leverages incorrect compiler optimization of an integer-overflow protection mechanism, aka Android internal bug 28821731 and Qualcomm internal bug CR691916. **Reference: CVE-2014-9799**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/344
Denial of Service	2016-07-10	7.1	platform/msm_shared/dev_tree.c in the Qualcomm bootloader in Android before 2016-07-05 on Nexus 5 devices does not check the relationship between tags addresses and aboot addresses, which allows attackers to cause a denial of service (OS outage) via a crafted application, aka Android internal bug 28821448 and Qualcomm internal bug CR681965. **Reference: CVE-2014-9798**	http://source.android.com/security/bulletin/2016-07-01.html	O-GOO-ANDRO-250716/345

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

IBM					
Websphere Datapower Xc10 Appliance Firmware *IBM WebSphere DataPower Appliances is a family of pre-built, pre-configured rack mountable network devices (XML appliances) that can help accelerate XML and Web Services deployments while extending SOA infrastructure.*					
Bypass	2016-07-10	9.3	app/aboot/aboot.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate the page size in the kernel header, which allows attackers to bypass intended access restrictions via a crafted boot image, aka Android internal bug 28820722 and Qualcomm internal bug CR684756. **Reference: CVE-2014-9796**	http://source.android.com/security/bulletin/2016-07-01.html	O-IBM-WEBSP-250716/346
Linux					
Linux Kernel *The Linux kernel is a Unix-like computer operating system kernel.*					
Overflow Bypass	2016-07-10	10	app/aboot/aboot.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices does not properly check for an integer overflow, which allows attackers to bypass intended access restrictions via crafted start and size values, aka Android internal bug 28820720 and Qualcomm internal bug CR681957, a related issue to CVE-2014-4325. **Reference: CVE-2014-9795**	http://source.android.com/security/bulletin/2016-07-01.html	O-LIN-LINUX-250716/347
Microsoft					
Windows 10 *Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft*					
Gain Privileges	2016-07-10	9.3	platform/msm_shared/mmc.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices mishandles the power-on write-protect feature, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28821253 and Qualcomm internal bug CR580567.	http://source.android.com/security/bulletin/2016-07-01.html	O-MIC-WINDO-250716/348

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-2014-9793		
Windows 10; Windows 7; Windows 8.1; Windows Rt 8.1;Windows Server 2008; Windows Server 2012; Windows Vista *Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft; Windows RT is a discontinued operating system for mobile devices developed by Microsoft. It is essentially an edition of Windows 8.x built for the 32-bit ARM architecture (ARMv7).*					
Gain Privileges	2016-07-10	9.3	arch/arm/mach-msm/ipc_router.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices uses an incorrect integer data type, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28769399 and Qualcomm internal bug CR550606. **Reference: CVE-2014-9792**	http://source.android.com/security/bulletin/2016-07-01.html	O-MIC-WINDO-250716/349
Gain Privileges	2016-07-10	9.3	drivers/mmc/core/debugfs.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate pointers used in read and write operations, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28769136 and Qualcomm internal bug CR545716. **Reference: CVE-2014-9790**	http://source.android.com/security/bulletin/2016-07-01.html	O-MIC-WINDO-250716/350
Gain Privileges	2016-07-10	9.3	The (1) alloc and (2) free APIs in arch/arm/mach-msm/qdsp6v2/msm_audio_ion.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices do not validate parameters, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28749392 and Qualcomm internal bug CR556425. **Reference: CVE-2014-9789**	http://source.android.com/security/bulletin/2016-07-01.html	O-MIC-WINDO-250716/351
Overflow; Gain Privileges	2016-07-10	9.3	Multiple buffer overflows in the voice drivers in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices	http://source.android.com/security/bulletin/2016-07-01.html	O-MIC-WINDO-250716/352

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

			allow attackers to gain privileges via a crafted application, aka Android internal bug 28573112 and Qualcomm internal bug CR548872. **Reference: CVE-2014-9788**		
Overflow; Gain Privileges	2016-07-10	9.3	Integer overflow in drivers/misc/qseecom.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28571496 and Qualcomm internal bug CR545764. **Reference: CVE-2014-9787**	http://source.android.com/security/bulletin/2016-07-01.html	O-MIC-WINDO-250716/353
Overflow; Gain Privileges	2016-07-10	9.3	Heap-based buffer overflow in drivers/media/platform/msm/camera_v2/sensor/actuator/msm_actuator.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28557260 and Qualcomm internal bug CR545979. **Reference: CVE-2014-9786**	http://source.android.com/security/bulletin/2016-07-01.html	O-MIC-WINDO-250716/354
Gain Privileges	2016-07-10	9.3	drivers/misc/qseecom.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices does not validate addresses before copying data, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28469042 and Qualcomm internal bug CR545747. **Reference: CVE-2014-9785**	http://source.android.com/security/bulletin/2016-07-01.html	O-MIC-WINDO-250716/355
Windows 10; Windows 7; Windows Rt 8.1; Windows Server 2012 *Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft; Windows RT is a discontinued operating system for mobile devices developed by Microsoft. It is essentially an edition of Windows 8.x built for the 32-bit ARM architecture (ARMv7).*					
Overflow; Gain Privileges	2016-07-10	9.3	Multiple buffer overflows in drivers/char/diag/diag_debugfs.c in the Qualcomm	http://source.android.com/security/bulletin/201	O-MIC-WINDO-250716/356

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

			components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allow attackers to gain privileges via a crafted application, aka Android internal bug 28442449 and Qualcomm internal bug CR585147. **Reference: CVE-2014-9784**	6-07-01.html	
Gain Privileges	2016-07-10	9.3	drivers/media/platform/msm/camera_v2/sensor/cci/msm_cci.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices does not validate certain values, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28441831 and Qualcomm internal bug CR511382. **Reference: CVE-2014-9783**	http://source.android.com/security/bulletin/2016-07-01.html	O-MIC-WINDO-250716/357
Gain Privileges	2016-07-10	9.3	drivers/media/platform/msm/camera_v2/sensor/actuator/msm_actuator.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate direction and step parameters, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28431531 and Qualcomm internal bug CR511349. **Reference: CVE-2014-9782**	http://source.android.com/security/bulletin/2016-07-01.html	O-MIC-WINDO-250716/358
Overflow; Gain Privileges	2016-07-10	9.3	Buffer overflow in drivers/video/fbcmap.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28410333 and Qualcomm internal bug CR556471. **Reference: CVE-2014-9781**	http://source.android.com/security/bulletin/2016-07-01.html	O-MIC-WINDO-250716/359
Ntt East					
Pr-400mi Firmware; Rt-400mi Firmware; Rv-440mi Firmware **NA**					

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

Gain Privileges	2016-07-10	9.3	drivers/video/msm/mdss/mdp3_ctrl.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5, 5X, and 6P devices does not validate start and length values, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28602014 and Qualcomm internal bug CR542222. **Reference: CVE-2014-9780**	http://source.android.com/security/bulletin/2016-07-01.html	O-NTT-PR-40-250716/360
Paloaltonetworks					
Pan-os *Pan-os is a discontinued computer operating system developed by Acorn Computers in the 1980s, which ran on the 32016 Second Processor for the BBC Micro and the Acorn Cambridge Workstation.*					
Gain Information	2016-07-10	9.3	arch/arm/mach-msm/qdsp6v2/msm_audio_ion.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices allows attackers to obtain sensitive information from kernel memory via a crafted offset, aka Android internal bug 28598347 and Qualcomm internal bug CR548679. **Reference: CVE-2014-9779**	http://source.android.com/security/bulletin/2016-07-01.html	O-PAL-PAN-O-250716/361
Qnap					
QTS *Quality Technology Services provides a wide range of data center services.*					
Overflow; Gain Privileges	2016-07-10	9.3	The vid_dec_set_h264_mv_buffers function in drivers/video/msm/vidc/common/dec/vdec.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate the number of buffers, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28598515 and Qualcomm internal bug CR563694. **Reference: CVE-2014-9778**	http://source.android.com/security/bulletin/2016-07-01.html	O-QNA-QTS-250716/362
Schneider-electric					

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

Pelco Digital Sentry Video Management System Firmware *With full-featured DS NVS video management software, the convenience and assurance of a robust network video recorder (DSSRV-2), analog camera support via optional direct-attached or network video encoders, and support for hundreds of IP cameras, Digital Sentry (DS) offers the flexibility and convenience of a video management system optimized to drive HD, IP, and hybrid recording from one high-performance platform.*					
Overflow; Gain Privileges	2016-07-10	9.3	The vid_dec_set_meta_buffers function in drivers/video/msm/vidc/common/dec/vdec.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate the number of buffers, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28598501 and Qualcomm internal bug CR563654. **Reference: CVE-2014-9777**	http://source.android.com/security/bulletin/2016-07-01.html	O-SCH-PELCO-250716/363
Somachine Hvac Firmware *SoMachine is a unique solution software for developing, configuring, and commissioning the entire machine in a single software environment.*					
Gain Privileges	2016-07-10	10	Unspecified vulnerability in the Qualcomm components in Android before 2016-07-05 allows attackers to gain privileges via a crafted application. **Reference: CVE-2013-7457**	http://source.android.com/security/bulletin/2016-07-01.html	O-SCH-SOMAC-250716/364

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