National Critical Information Infrastructure Protection Centre

CVE Report

01 – 15 June 2016

Vol. 03 No.10

Vulnerability Type	Publish Date	CVSS	Vulnerability Description	Patch	NCIIPC ID
OS					
Sixnet					
Bt-5 Series Cellular Router Firmware;Bt-6 Series Cellular Router Firmware:					
+Info	2016-05-30	10	Sixnet BT-5xxx and BT-6xxx M2M devices before 3.8.21 and 3.9.x before 3.9.8 have hardcoded credentials, which allows remote attackers to obtain access via unspecified vectors. **Reference:** CVE-2016-4521	https://ics-cert.us-cert.gov/advisories/ICSA-16-147-02	O-SIX-BT-5-270616/1
Application					
Resourcedm					
Intuitive 650 Tdb Controller: Intuitive TDB controllers can facilitate the most demanding HVACR and BEMS applications.					
CSRF	2016-05-30	6	Cross-site request forgery (CSRF) vulnerability on Resource Data Management (RDM) Intuitive 650 TDB Controller devices before 2.1.24 allows remote authenticated users to hijack the authentication of arbitrary users. **Reference:** CVE-2016-4506	https://ics-cert.us-cert.gov/advisories/ICSA-16-140-01	A-RES-INTUI-270616/2
NA	2016-05-30	9	Resource Data Management (RDM) Intuitive 650 TDB Controller devices before 2.1.24 allow remote authenticated users to modify arbitrary passwords via unspecified vectors. **Reference:** CVE-2016-4505	https://ics-cert.us-cert.gov/advisories/ICSA-16-140-01	A-RES-INTUI-270616/3
Envirosys					
Esc 8832 Data Controller: An ESC Data Controller bridges the gap between the measurement analyzers in the CEMS rack and the ESC|StackVision server.					
Bypass	2016-05-30	5	Environmental Systems Corporation (ESC) 8832 Data Controller 3.02 and earlier allows remote attackers to bypass intended access restrictions and execute arbitrary functions via a modified parameter. **Reference:** CVE-2016-4502	https://ics-cert.us-cert.gov/advisories/ICSA-16-147-01	A-ENV-ESC 8-270616/4
Bypass	2016-05-30	6.4	Environmental Systems Corporation (ESC) 8832 Data Controller 3.02 and	https://ics-cert.us-cert.gov/advisories/ICSA-	A-ENV-ESC

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

			earlier mishandles sessions, which allows remote attackers to bypass authentication and make arbitrary configuration changes via unspecified vectors. **Reference:** CVE-2016-4501	16-147-01	8-270616/5
OS					
Moxa					
Miineport E1 4641 Firmware;Miineport E1 7080 Firmware;Miineport E2 1242 Firmware;Miineport E2 4561 Firmware;Miineport E3 Firmware: MiiNePort E1-SDK is a powerful and versatile software suite for proprietary firmware development on the MiiNePort E1.					
+Info		5	Moxa MiiNePort_E1_4641 devices with firmware 1.1.10 Build 09120714, MiiNePort_E1_7080 devices with firmware 1.1.10 Build 09120714, MiiNePort_E2_1242 devices with firmware 1.1 Build 10080614, MiiNePort_E2_4561 devices with firmware 1.1 Build 10080614, and MiiNePort E3 devices with firmware 1.0 Build 11071409 allow remote attackers to obtain sensitive cleartext information by reading a configuration file. **Reference:** CVE-2016-2295	https://ics-cert.us-cert.gov/advisories/ICSA-16-145-01	O-MOX-MIINE-270616/6
NA	2016-05-30	5	Moxa MiiNePort_E1_4641 devices with firmware 1.1.10 Build 09120714, MiiNePort_E1_7080 devices with firmware 1.1.10 Build 09120714, MiiNePort_E2_1242 devices with firmware 1.1 Build 10080614, MiiNePort_E2_4561 devices with firmware 1.1 Build 10080614, and MiiNePort E3 devices with firmware 1.0 Build 11071409 have a blank default password, which allows remote attackers to obtain access via unspecified vectors. **Reference:** CVE-2016-2286	https://ics-cert.us-cert.gov/advisories/ICSA-16-145-01	O-MOX-MIINE-270616/7
CSRF	2016-05-30	6.8	Cross-site request forgery (CSRF) vulnerability on Moxa MiiNePort_E1_4641 devices with firmware 1.1.10 Build 09120714, MiiNePort_E1_7080 devices with firmware 1.1.10 Build 09120714, MiiNePort_E2_1242 devices with firmware 1.1 Build 10080614, MiiNePort_E2_4561 devices with firmware 1.1 Build 10080614, and MiiNePort E3 devices with firmware 1.0 Build 11071409 allows remote attackers to hijack the authentication of arbitrary users. **Reference:** CVE-2016-2285	https://ics-cert.us-cert.gov/advisories/ICSA-16-145-01	O-MOX-MIINE-270616/8

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

Sixnet					
Bt-5 Series Cellular Router Firmware;Bt-6 Series Cellular Router Firmware: NA					
+Info	2016-05-30	10	Sixnet BT-5xxx and BT-6xxx M2M devices before 3.8.21 and 3.9.x before 3.9.8 have hardcoded credentials, which allows remote attackers to obtain access via unspecified vectors. **Reference:** CVE-2016-4521	https://ics-cert.us-cert.gov/advisories/ICSA-16-147-02	O-SIX-BT-5-270616/9
Application					
Qemu					
Qemu: QEMU (short for Quick Emulator) is a free and open-source hosted hypervisor that performs hardware virtualization QEMU is a hosted virtual machine monitor					
DoS Exec Code Overflow	2016-06-01	4.6	Heap-based buffer overflow in the iscsi_aio_ioctl function in block/iscsi.c in QEMU allows local guest OS users to cause a denial of service (QEMU process crash) or possibly execute arbitrary code via a crafted iSCSI asynchronous I/O ioctl call. **Reference:** CVE-2016-5126	http://git.qemu.org/?p=qemu.git;a=commit;h=a6b3167fa0e825aebb5a7cd8b437b6d41584a196	A-QEM-QEMU-270616/10
OS					
Netscaler Gateway 11.0 Firmware: NetScaler is a hardware device (or network appliance) manufactured by Citrix, which primary role is to provide Level 4 Load Balancing.					
XSS	2016-06-01	4.3	Cross-site scripting (XSS) vulnerability in vpn/js/gateway_login_form_view.js in Citrix NetScaler Gateway 11.0 before Build 66.11 allows remote attackers to inject arbitrary web script or HTML via the NSC_TMAC cookie. **Reference:** CVE-2016-4945	http://support.citrix.com/article/CTX213313	O-CIT-NETSC-270616/11
Application					
Citrix					
Xenapp;Xendesktop: Citrix XenApp is a product that extends Microsoft Remote Desktop Session Host (formerly known as "Terminal Services") desktop sessions and applications to users through the Citrix HDX protocol.					
NA	2016-06-01	5	Citrix Studio before 7.6.1000, Citrix XenDesktop 7.x before 7.6 LTSR Cumulative Update 1 (CU1), and Citrix XenApp 7.5 and 7.6 allow attackers to set Access Policy rules on the XenDesktop Delivery Controller via unspecified vectors. **Reference:** CVE-2016-4810	http://support.citrix.com/article/CTX213045	A-CIT-XENAP-270616/12

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

Hardware/OS					
Moxa					
Uc-7408 Lx-plus/Uc-7408 Lx-plus Firmware: UC-7408-LX-Plus, is an embedded computer.					
NA	2016-06-01	4.9	Moxa UC-7408 LX-Plus devices allow remote authenticated users to write to the firmware, and consequently render a device unusable, by leveraging root access. **Reference:** CVE-2016-4500	https://ics-cert.us-cert.gov/advisories/ICSA-16-152-01	H-MOX-UC-74-270616/13
Application					
Qemu					
Qemu: QEMU (short for Quick Emulator) is a free and open-source hosted hypervisor that performs hardware virtualization QEMU is a hosted virtual machine monitor					
DoS Overflow +Info	2016-06-01	3.2	The vmsvga_fifo_read_raw function in hw/display/vmware_vga.c in QEMU allows local guest OS administrators to obtain sensitive host memory information or cause a denial of service (QEMU process crash) by changing FIFO registers and issuing a VGA command, which triggers an out-of-bounds read. **Reference:** CVE-2016-4454	https://bugzilla.redhat.com/show_bug.cgi?id=1336429	A-QEM-QEMU-270616/14
DoS	2016-06-01	4.6	The vmsvga_fifo_run function in hw/display/vmware_vga.c in QEMU allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via a VGA command. **Reference:** CVE-2016-4453	https://bugzilla.redhat.com/show_bug.cgi?id=1336650	A-QEM-QEMU-270616/15
Apache					
Qpid Java: A message-oriented middleware message broker written in Java that stores, routes, and forwards messages using AMQP.					
Bypass	2016-06-01	5	The AMQP 0-8, 0-9, 0-91, and 0-10 connection handling in Apache Qpid Java before 6.0.3 might allow remote attackers to bypass authentication and consequently perform actions via vectors related to connection state logging. **Reference:** CVE-2016-4432	https://svn.apache.org/viewvc?view=revision&revision=1743393	A-APA-QPID -270616/16
OS/Application					
Debian/Sensiolabs					
Debian Linux/Symfony: Debian is an operating system and a distribution of Free Software. Symfony is a set of reusable PHP components					
DoS	2016-06-01	5	The attemptAuthentication function in Component/Security/Http/Firewall/UsernamePasswordFormAuthenticationListener.php in Symfony before 2.3.41, 2.7.x before 2.7.13, 2.8.x before 2.8.6,	https://symfony.com/blog/cve-2016-4423-large-username-storage-in-session	O-DEB-DEBIA-270616/17

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

			and 3.0.x before 3.0.6 does not limit the length of a username stored in a session, which allows remote attackers to cause a denial of service (session storage consumption) via a series of authentication attempts with long, non-existent usernames. **Reference:** CVE-2016-4423		
Application;OS					
Docker;Open Container Project					
Docker/Runc/Opensuse: Docker is an open platform for developers and sysadmins to build, ship, and run distributed applications, whether on laptops, data center VMs, or the cloud. Runc is a lightweight universal runtime container. openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.					
+Priv	2016-06-01	2.1	libcontainer/user/user.go in runC before 0.1.0, as used in Docker before 1.11.2, improperly treats a numeric UID as a potential username, which allows local users to gain privileges via a numeric username in the password file in a container. **Reference:** CVE-2016-3697	https://github.com/opencontainers/runc/releases/tag/v0.1.0	A-DOC-DOCKE-270616/18
Application					
Apache					
Qpid Java: A message-oriented middleware message broker written in Java that stores, routes, and forwards messages using AMQP.					
DoS	2016-06-01	4.3	PlainSaslServer.java in Apache Qpid Java before 6.0.3, when the broker is configured to allow plaintext passwords, allows remote attackers to cause a denial of service (broker termination) via a crafted authentication attempt, which triggers an uncaught exception. **Reference:** CVE-2016-3094	http://qpid.apache.org/releases/qpid-java-6.0.3/release-notes.html	A-APA-QPID -270616/19
Activemq: A complete message broker and full JMS 1.1 provider featuring clustering, distributed destinations and XA support with pluggable persistence					
NA	2016-06-01	7.5	The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0 allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request. **Reference:** CVE-2016-3088	http://activemq.apache.org/security-advisories.data/CVE-2016-3088-announcement.txt	A-APA-ACTIV-270616/20
OS/Application					
Canonical;Fedoraproject/GNU					
Ubuntu Linux/Fedora/Glibc: Ubuntu is an open source software platform that runs everywhere from the smartphone. Fedora is a Linux based operating system. The GNU C Library, commonly known as glibc, is the GNU Project's implementation of the C standard library. Despite its name, it now also directly supports C++ (and, indirectly,					

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

other programming languages).					
DoS Overflow	2016-06-01	5	Stack-based buffer overflow in the nss_dns implementation of the getnetbyname function in GNU C Library (aka glibc) before 2.24 allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a long name. **Reference:** CVE-2016-3075	https://sourceware.org/git/gitweb.cgi?p=glibc.git;h=317b199b4aff8cfa27f2302ab404d2bb5032b9a4	O-CAN-UBUNT-270616/21
Application					
Apache					
Pdfbox: The Apache PDFBox library is an open source Java tool for working with PDF documents					
NA	2016-06-01	7.5	Apache PDFBox before 1.8.12 and 2.x before 2.0.1 does not properly initialize the XML parsers, which allows context-dependent attackers to conduct XML External Entity (XXE) attacks via a crafted PDF. **Reference:** CVE-2016-2175	http://svn.apache.org/viewvc?view=revision&revision=1739564	A-APA-PDFBO-270616/22
OS/Application					
Debian/Sensiolabs					
Debian Linux/Symfony: Debian is an operating system and a distribution of Free Software. Symfony is a set of reusable PHP components					
NA	2016-06-01	5	The nextBytes function in the SecureRandom class in Symfony before 2.3.37, 2.6.x before 2.6.13, and 2.7.x before 2.7.9 does not properly generate random numbers when used with PHP 5.x without the paragonie/random_compat library and the openssl_random_pseudo_bytes function fails, which makes it easier for attackers to defeat cryptographic protection mechanisms via unspecified vectors. **Reference:** CVE-2016-1902	https://github.com/symfony/symfony/pull/17359	O-DEB-DEBIA-270616/23
Fedoraproject;Novell/GNU					
Fedora/Opensuse/Glibc: Fedora is a A Linux based operating system. openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.The GNU C Library, commonly known as glibc, is the GNU Project's implementation of the C standard library. Despite its name, it now also directly supports C++ (and, indirectly, other programming languages).					
DoS Overflow	2016-06-01	5	Stack-based buffer overflow in the glob implementation in GNU C Library (aka glibc) before 2.24, when GLOB_ALTDIRFUNC is used, allows context-dependent attackers to cause a denial of service (crash) via a long name. **Reference:** CVE-2016-1234	https://sourceware.org/git/gitweb.cgi?p=glibc.git;h=5171f3079f2cc53e0548fc4967361f4d1ce9d7ea	O-FED-FEDOR-270616/24
Application					
IBM					
Security Appscan: IBM Security AppScan, previously known as IBM Rational AppScan, is a family of web security testing and monitoring					

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

tools.					
NA	2016-06-01	4	IBM Security AppScan Standard 8.7.x, 8.8.x, and 9.x before 9.0.3.2 and Security AppScan Enterprise allow remote authenticated users to read arbitrary files via an XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. **Reference:** CVE-2016-0288	http://www-01.ibm.com/support/docview.wss?uid=swg21980055	A-IBM-SECUR-270616/25
OS;Application					
Debian/Gnome					
Debian Linux/Gdk-pixbuf: Debian is an operating system and a distribution of Free Software. Symfony is a set of reusable PHP components. GdkPixbuf is a library for image loading and manipulation.					
DoS Exec Code Overflow	2016-06-01	6.8	Multiple integer overflows in the (1) pixops_composite_nearest, (2) pixops_composite_color_nearest, and (3) pixops_process functions in pixops/pixops.c in gdk-pixbuf before 2.33.1 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted image, which triggers a heap-based buffer overflow. **Reference:** CVE-2015-8875	https://git.gnome.org/browse/gdk-pixbuf/commit/?id=dbfe8f70471864818bf458a39c8a99640895bd22	O-DEB-DEBIA-270616/26
Hardware;OS					
Cisco/Cisco					
Network Analysis Module/Prime Network Analysis Module Software; Prime Virtual Network Analysis Module Software: The Cisco Network Analysis Module products deliver pervasive visibility to help you gain better control.					
Exec Code	2016-06-02	7.5	Cisco Prime Network Analysis Module (NAM) before 6.1(1) patch.6.1-2-final and 6.2.x before 6.2(1) and Prime Virtual Network Analysis Module (vNAM) before 6.1(1) patch.6.1-2-final and 6.2.x before 6.2(1) allow remote attackers to execute arbitrary OS commands via a crafted HTTP request, aka Bug ID CSCuy21882. **Reference:** CVE-2016-1388	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160601-prime	H-CIS-NETWO-270616/27
OS					
CISCO					
Network Analysis Module Software: The Cisco Network Analysis Module products deliver pervasive visibility to help you gain better control.					
DoS	2016-06-02	5	Cisco Prime Network Analysis Module (NAM) before 6.2(1-b) miscalculates IPv6 payload lengths, which allows remote attackers to cause a denial of service (mond process crash and monitoring outage) via crafted IPv6 packets, aka Bug ID CSCuy37324. **Reference:** CVE-2016-1370	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160601-prime3	O-CIS-NETWO-270616/28

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

OS;Application

Canonical;Novell/Dosfstools Project

Ubuntu Linux/Leap;Opensuse/Dosfstools:

Ubuntu is an open source software platform. dosfstools consists of the programs mkfs.fat, fsck.fat and fatlabel to create, check and label file systems of the FAT family.

DoS Overflow	2016-06-03	2.1	The read_boot function in boot.c in dosfstools before 4.0 allows attackers to cause a denial of service (crash) via a crafted filesystem, which triggers a heap-based buffer overflow in the (1) read_fat function or an out-of-bounds heap read in (2) get_fat function. **Reference:** CVE-2016-4804	https://github.com/dosfstools/dosfstools/issues/25	O-CAN-UBUNT-270616/29

Application

Lenovo

Accelerator Application:

Advanced Accelerator Applications Expands U.S. NETSPOT™ Supply Chain with Two Additional Radiopharmacy Networks

Exec Code	2016-06-03	9.3	UpdateAgent in Lenovo Accelerator Application allows man-in-the-middle attackers to execute arbitrary code by spoofing an update response from susapi.lenovomm.com. **Reference:** CVE-2016-3944	https://support.lenovo.com/us/en/product_security/len_6718	A-LEN-ACCEL-270616/30

Application;OS

Ansibleworks/Fedoraproject

Ansible/Fedora:

Ansible is the simplest way to automate apps and IT infrastructure. Fedora is a A Linux based operating system.

+Priv	2016-06-03	7.2	The create_script function in the lxc_container module in Ansible before 1.9.6-1 and 2.x before 2.0.2.0 allows local users to write to arbitrary files or gain privileges via a symlink attack on (1) /opt/.lxc-attach-script, (2) the archived container in the archive_path directory, or the (3) lxc-attach-script.log or (4) lxc-attach-script.err files in the temporary directory. **Reference:** CVE-2016-3096	https://bugzilla.redhat.com/show_bug.cgi?id=1322925	A-ANS-ANSIB-270616/31

OS

Cisco

Prime Network Analysis Module Software;Prime Virtual Network Analysis Module Software:

The Cisco Network Analysis Module products deliver pervasive visibility to help you gain better control.

Exec Code	2016-06-03	6.5	Cisco Prime Network Analysis Module (NAM) before 6.1(1) patch.6.1-2-final and 6.2.x before 6.2(2) and Prime Virtual Network Analysis Module (vNAM) before 6.1(1) patch.6.1-2-final and 6.2.x before 6.2(2) allow remote authenticated users to execute arbitrary OS commands via a crafted HTTP request, aka Bug ID CSCuy21889. **Reference:** CVE-2016-1391	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160601-prime2	O-CIS-PRIME-270616/32

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

Application

Cisco

Prime Network Analysis Module Software;Prime Virtual Network Analysis Module Software:

The Cisco Network Analysis Module products deliver pervasive visibility to help you gain better control.

NA	2016-06-03	7.2	Cisco Prime Network Analysis Module (NAM) before 6.1(1) patch.6.1-2-final and 6.2.x before 6.2(1) and Prime Virtual Network Analysis Module (vNAM) before 6.1(1) patch.6.1-2-final and 6.2.x before 6.2(1) allow local users to obtain root access via crafted CLI input, aka Bug ID CSCuy21892. **Reference:** CVE-2016-1390	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160601-prime1	A-CIS-PRIME-270616/33

OS

EMC

Isilon Onefs:

EMC Isilon OneFS operating system provides the intelligence behind EMC Isilon scale-out NAS storage solutions.

NA	2016-06-03	6.8	EMC Isilon OneFS 7.1.x before 7.1.1.9 and 7.2.x before 7.2.1.2 allows local users to obtain root shell access by leveraging administrative privileges. **Reference:** CVE-2016-0908	http://seclists.org/bugtraq/2016/Jun/13	O-EMC-ISILO-270616/34

Application;OS

IBM/Novell;Redhat

Java Sdk/Suse Linux Enterprise Module For Legacy Software;Suse Linux Enterprise Server;Suse Linux Enterprise Software Development Kit;Suse Manager;Suse Manager Proxy;Suse Openstack Cloud/Enterprise Linux Desktop Supplementary;Enterprise Linux Hpc Node Supplementary;Enterprise Linux Server Supplementary;Enterprise Linux Server Supplementary Eus;Enterprise Linux Supplementary;Enterprise Linux Workstation Supplementary:

The Java Development Kit is a collection of tools that developers use to deploy applications written in Java.

Exec Code Bypass	2016-06-03	5.1	The com.ibm.rmi.io.SunSerializableFactory class in IBM SDK, Java Technology Edition 6 before SR16 FP25 (6.0.16.25), 6 R1 before SR8 FP25 (6.1.8.25), 7 before SR9 FP40 (7.0.9.40), 7 R1 before SR3 FP40 (7.1.3.40), and 8 before SR3 (8.0.3.0) does not properly deserialize classes in an AccessController doPrivileged block, which allows remote attackers to bypass a sandbox protection mechanism and execute arbitrary code as demonstrated by the readValue method of the com.ibm.rmi.io.ValueHandlerPool.ValueHandlerSingleton class, which implements the javax.rmi.CORBA.ValueHandler interface. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-5456. **Reference:** CVE-2016-0376	http://www-01.ibm.com/support/docview.wss?uid=swg21980826	A-IBM-JAVA - 270616/35

Application;OS

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

IBM/Novell;Redhat					
Java Sdk/Suse Linux Enterprise Module For Legacy Software;Suse Linux Enterprise Server;Suse Linux Enterprise Software Development Kit;Suse Manager;Suse Manager Proxy;Suse Openstack Cloud/Enterprise Linux Desktop Supplementary;Enterprise Linux Hpc Node Supplementary;Enterprise Linux Server Supplementary;Enterprise Linux Server Supplementary Eus;Enterprise Linux Supplementary;Enterprise Linux Workstation Supplementary: The Java Development Kit is a collection of tools that developers use to deploy applications written in Java.					
Bypass	2016-06-03	6.8	The com.ibm.CORBA.iiop.ClientDelegate class in IBM SDK, Java Technology Edition 6 before SR16 FP25 (6.0.16.25), 6 R1 before SR8 FP25 (6.1.8.25), 7 before SR9 FP40 (7.0.9.40), 7 R1 before SR3 FP40 (7.1.3.40), and 8 before SR3 (8.0.3.0) uses the invoke method of the java.lang.reflect.Method class in an AccessController doPrivileged block, which allows remote attackers to call setSecurityManager and bypass a sandbox protection mechanism via vectors related to a Proxy object instance implementing the java.lang.reflect.InvocationHandler interface. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-3009. **Reference:** CVE-2016-0363	http://www-01.ibm.com/support/docview.wss?uid=swg21980826	A-IBM-JAVA -270616/36
OS;Application					
Canonical;Novell/Dosfstools Project					
Ubuntu Linux/Leap;Opensuse/Dosfstools: Ubuntu is an open source software platform. dosfstools consists of the programs mkfs.fat, fsck.fat and fatlabel to create, check and label file systems of the FAT family.					
DoS	2016-06-03	2.1	The set_fat function in fat.c in dosfstools before 4.0 might allow attackers to corrupt a FAT12 filesystem or cause a denial of service (invalid memory read and crash) by writing an odd number of clusters to the third to last entry on a FAT12 filesystem, which triggers an "off-by-two error." **Reference:** CVE-2015-8872	https://github.com/dosfstools/dosfstools/releases/tag/v4.0	O-CAN-UBUNT-270616/37
Application					
Markdown On Saved Improved Project					
Markdown On Saved Improved: NA					
XSS	2016-06-04	4.3	Cross-site scripting (XSS) vulnerability in the Markdown on Save Improved plugin before 2.5.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference:** CVE-2016-4812	https://srd.wordpress.org/plugins/markdown-on-save-improved/changelog/	A-MAR-MARKD-270616/38

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

Imagemagick					
Imagemagick: ImageMagick® is a software suite to create, edit, compose, or convert bitmap images.					
DoS Overflow	2016-06-04	7.5	The DrawImage function in MagickCore/draw.c in ImageMagick before 6.9.4-0 and 7.x before 7.0.1-2 makes an incorrect function call in attempting to locate the next token, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted file. **Reference:** CVE-2016-4564	https://github.com/ImageMagick/ImageMagick/commit/726812fa2fa7ce16bcf58f6e115f65427a1c0950	A-IMA-IMAGE-270616/39
DoS Overflow	2016-06-04	6.8	The TraceStrokePolygon function in MagickCore/draw.c in ImageMagick before 6.9.4-0 and 7.x before 7.0.1-2 mishandles the relationship between the BezierQuantum value and certain strokes data, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted file. **Reference:** CVE-2016-4563	https://github.com/ImageMagick/ImageMagick/commit/726812fa2fa7ce16bcf58f6e115f65427a1c0950	A-IMA-IMAGE-270616/40
DoS Overflow	2016-06-04	6.8	The DrawDashPolygon function in MagickCore/draw.c in ImageMagick before 6.9.4-0 and 7.x before 7.0.1-2 mishandles calculations of certain vertices integer data, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted file. **Reference:** CVE-2016-4562	https://github.com/ImageMagick/ImageMagick/commit/726812fa2fa7ce16bcf58f6e115f65427a1c0950	A-IMA-IMAGE-270616/41
OS					
Cisco					
Ip Phone 8800 Series Firmware: NA					
Exec Code +Priv	2016-06-04	7.2	CISCO IP 8800 phones with software 11.0.1 and earlier allow local users to gain privileges for OS command execution via crafted CLI commands, aka Bug ID CSCuz03005. **Reference:** CVE-2016-1403	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160603-ipp	O-CIS-IP PH-270616/42
Application					
NTT					
Webarena Service Formmail: NA					
XSS	2016-06-04	4.3	Cross-site scripting (XSS) vulnerability in NTT PC Communications WebARENA Service formmail before 2.2.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference:** CVE-2016-1230	http://web.arena.ne.jp/support/news/2016/0208.html	A-NTT-WEBAR-270616/43

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

Humhub					
Humhub: HumHub is a free social network software and framework built to give you the tools to make teamwork easy and successful.					
XSS	2016-06-04	3.5	Cross-site scripting (XSS) vulnerability in HumHub 0.20.0-beta.1 through 0.20.1 and 1.0.0-beta before 1.0.0-beta.3 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference:** CVE-2016-1229	https://github.com/humhub/humhub/releases/tag/v1.0.0-beta.3	A-HUM-HUMHU-270616/44
Kobe-beauty					
Php-contact-form: PHP contact form script code that allows website owners to let visitors contact them by email, without revealing their email address on the web page.					
XSS	2016-06-04	4.3	Cross-site scripting (XSS) vulnerability in Kobe Beauty php-contact-form before 2016-05-18 allows remote attackers to inject arbitrary web script or HTML via a crafted URI. **Reference:** CVE-2016-1222	https://github.com/kobebeauty/php-contact-form/commit/e7d094ca8ab15215c32d6fa04d17e8519c8d21cf	A-KOB-PHP-C-270616/45
Futomi					
Mp Form Mail Cgi: NA					
Dir. Trav.	2016-06-04	4	Directory traversal vulnerability in futomi MP Form Mail CGI Professional Edition 3.2.3 and earlier allows remote authenticated administrators to read arbitrary files via unspecified vectors. **Reference:** CVE-2016-1212	http://www.futomi.com/library/info/2016/201605.html	A-FUT-MP FO-270616/46
Epoch					
Web Mailing List: To Create and send email newsletters with ease.					
XSS	2016-06-04	4.3	Cross-site scripting (XSS) vulnerability in Epoch Web Mailing List 0.31 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference:** CVE-2016-1211	http://www.psl.ne.jp/perl/ml/index.html	A-EPO-WEB M-270616/47
Google					
Chrome: Google Chrome is a browser that combines a minimal design with sophisticated technology to make the web faster, safer, and easier.					
DoS	2016-06-05	6.8	Multiple unspecified vulnerabilities in Google Chrome before 51.0.2704.79 allow attackers to cause a denial of service or possibly have other impact via unknown vectors. **Reference:** CVE-2016-1703	http://googlechromereleases.blogspot.com/2016/06/stable-channel-update.html	A-GOO-CHROM-270616/48
DoS Overflow	2016-	4.3	The SkRegion::readFromMemory function in	https://crbug.c	A-GOO-

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

	06-05		core/SkRegion.cpp in Skia, as used in Google Chrome before 51.0.2704.79, does not validate the interval count, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted serialized data. **Reference:** CVE-2016-1702	om/609260	CHROM-270616/49
DoS	2016-06-05	6.8	The Autofill implementation in Google Chrome before 51.0.2704.79 mishandles the interaction between field updates and JavaScript code that triggers a frame deletion, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site, a different vulnerability than CVE-2016-1690. **Reference:** CVE-2016-1701	https://crbug.com/608101	A-GOO-CHROM-270616/50
DoS	2016-06-05	5.1	extensions/renderer/runtime_custom_bindings.cc in Google Chrome before 51.0.2704.79 does not consider side effects during creation of an array of extension views, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to extensions. **Reference:** CVE-2016-1700	https://crbug.com/608104	A-GOO-CHROM-270616/51
Bypass	2016-06-05	4.3	WebKit/Source/devtools/front_end/devtools.js in the Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 51.0.2704.79, does not ensure that the remoteFrontendUrl parameter is associated with a chrome-devtools-frontend.appspot.com URL, which allows remote attackers to bypass intended access restrictions via a crafted URL. **Reference:** CVE-2016-1699	https://crbug.com/607939	A-GOO-CHROM-270616/52
+Info	2016-06-05	4.3	The createCustomType function in extensions/renderer/resources/binding.js in the extension bindings in Google Chrome before 51.0.2704.79 does not validate module types, which might allow attackers to load arbitrary modules or obtain sensitive information by leveraging a poisoned definition. **Reference:** CVE-2016-1698	https://crbug.com/603725	A-GOO-CHROM-270616/53
Bypass	2016-06-05	6.8	The FrameLoader::startLoad function in WebKit/Source/core/loader/FrameLoader.cpp in Blink, as used in Google Chrome before 51.0.2704.79, does not prevent frame navigations during DocumentLoader detach operations, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code. **Reference:** CVE-2016-1697	https://crbug.com/613266	A-GOO-CHROM-270616/54
Bypass	2016-06-05	6.8	The extensions subsystem in Google Chrome before 51.0.2704.79 does not properly restrict bindings access, which allows remote attackers to bypass the Same Origin Policy via unspecified vectors. **Reference:** CVE-2016-1696	https://crbug.com/601073	A-GOO-CHROM-270616/55
DoS	2016-06-05	6.8	Multiple unspecified vulnerabilities in Google Chrome before 51.0.2704.63 allow attackers to cause a denial of service or possibly have other	http://googlechromereleases.blogspot.com/20	A-GOO-CHROM-

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

			impact via unknown vectors. **Reference:** CVE-2016-1695	16/05/stable-channel-update_25.html	270616/56
NA	2016-06-05	4.3	browser/browsing_data/browsing_data_remover.cc in Google Chrome before 51.0.2704.63 deletes HPKP pins during cache clearing, which makes it easier for remote attackers to spoof web sites via a valid certificate from an arbitrary recognized Certification Authority. **Reference:** CVE-2016-1694	http://googlechromereleases.blogspot.com/2016/05/stable-channel-update_25.html	A-GOO-CHROM-270616/57
NA	2016-06-05	2.6	browser/safe_browsing/srt_field_trial_win.cc in Google Chrome before 51.0.2704.63 does not use the HTTPS service on dl.google.com to obtain the Software Removal Tool, which allows remote attackers to spoof the chrome_cleanup_tool.exe (aka CCT) file via a man-in-the-middle attack on an HTTP session. **Reference:** CVE-2016-1693	https://crbug.com/598752	A-GOO-CHROM-270616/58
Bypass	2016-06-05	4.3	WebKit/Source/core/css/StyleSheetContents.cpp in Blink, as used in Google Chrome before 51.0.2704.63, permits cross-origin loading of CSS stylesheets by a ServiceWorker even when the stylesheet download has an incorrect MIME type, which allows remote attackers to bypass the Same Origin Policy via a crafted web site. **Reference:** CVE-2016-1692	https://crbug.com/598077	A-GOO-CHROM-270616/59
DoS Overflow	2016-06-05	5.1	Skia, as used in Google Chrome before 51.0.2704.63, mishandles coincidence runs, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted curves, related to SkOpCoincidence.cpp and SkPathOpsCommon.cpp. **Reference:** CVE-2016-1691	https://crbug.com/597926	A-GOO-CHROM-270616/60
DoS	2016-06-05	5.1	The Autofill implementation in Google Chrome before 51.0.2704.63 mishandles the interaction between field updates and JavaScript code that triggers a frame deletion, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site, a different vulnerability than CVE-2016-1701. **Reference:** CVE-2016-1690	https://crbug.com/608100	A-GOO-CHROM-270616/61
DoS Overflow	2016-06-05	4.3	Heap-based buffer overflow in content/renderer/media/canvas_capture_handler.cc in Google Chrome before 51.0.2704.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site. **Reference:** CVE-2016-1689	https://crbug.com/606185	A-GOO-CHROM-270616/62
DoS Overflow	2016-06-05	4.3	The regexp (aka regular expression) implementation in Google V8 before 5.0.71.40, as used in Google Chrome before 51.0.2704.63, mishandles external string sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted JavaScript code. **Reference:** CVE-2016-1688	https://crbug.com/604897	A-GOO-CHROM-270616/63

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

+Info	2016-06-05	4.3	The renderer implementation in Google Chrome before 51.0.2704.63 does not properly restrict public exposure of classes, which allows remote attackers to obtain sensitive information via vectors related to extensions. **Reference:** CVE-2016-1687	https://crbug.com/603748	A-GOO-CHROM-270616/64
DoS Overflow	2016-06-05	4.3	The CPDF_DIBSource::CreateDecoder function in core/fpdfapi/fpdf_render/fpdf_render_loadimage.cpp in PDFium, as used in Google Chrome before 51.0.2704.63, mishandles decoder-initialization failure, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document. **Reference:** CVE-2016-1686	https://crbug.com/603518	A-GOO-CHROM-270616/65
DoS Overflow	2016-06-05	4.3	core/fxge/ge/fx_ge_text.cpp in PDFium, as used in Google Chrome before 51.0.2704.63, miscalculates certain index values, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document. **Reference:** CVE-2016-1685	https://crbug.com/601362	A-GOO-CHROM-270616/66
Google;Xmlsoft					
Chrome/Libxslt: Google Chrome is a browser that combines a minimal design with sophisticated technology to make the web faster, safer, and easier. Libxslt is the XSLT C library developed for the GNOME project.					
DoS Overflow	2016-06-05	5.1	numbers.c in libxslt before 1.1.29, as used in Google Chrome before 51.0.2704.63, mishandles the i format token for xsl:number data, which allows remote attackers to cause a denial of service (integer overflow or resource consumption) or possibly have unspecified other impact via a crafted document. **Reference:** CVE-2016-1684	https://git.gnome.org/browse/libxslt/commit/?id=91d0540ac9beaa86719a05b749219a69baa0dd8d	A-GOO-CHROM-270616/67
DoS Overflow	2016-06-05	5.1	numbers.c in libxslt before 1.1.29, as used in Google Chrome before 51.0.2704.63, mishandles namespace nodes, which allows remote attackers to cause a denial of service (out-of-bounds heap memory access) or possibly have unspecified other impact via a crafted document. **Reference:** CVE-2016-1683	https://git.gnome.org/browse/libxslt/commit/?id=d182d8f6ba3071503d96ce17395c9d55871f0242	A-GOO-CHROM-270616/68
Google					
Chrome: Google Chrome is a browser that combines a minimal design with sophisticated technology to make the web faster, safer, and easier.					
Bypass	2016-06-05	4.3	The ServiceWorkerContainer::registerServiceWorkerImpl function in WebKit/Source/modules/serviceworkers/ServiceWorkerContainer.cpp in Blink, as used in Google Chrome before 51.0.2704.63, allows remote attackers to bypass the Content Security Policy (CSP) protection mechanism via a ServiceWorker registration. **Reference:** CVE-2016-1682	https://crbug.com/579801	A-GOO-CHROM-270616/69
DoS Overflow	2016-06-05	6.8	Heap-based buffer overflow in the opj_j2k_read_SPCod_SPCoc function in j2k.c in	http://googlechromereleases.blogsp	A-GOO-CHROM-

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

			OpenJPEG, as used in PDFium in Google Chrome before 51.0.2704.63, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document. **Reference:** CVE-2016-1681	ot.com/2016/05/stable-channel-update_25.html	270616/70
DoS Overflow Mem. Corr.	2016-06-05	6.8	Use-after-free vulnerability in ports/SkFontHost_FreeType.cpp in Skia, as used in Google Chrome before 51.0.2704.63, allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via unknown vectors. **Reference:** CVE-2016-1680	https://crbug.com/589848	A-GOO-CHROM-270616/71
DoS	2016-06-05	6.8	The ToV8Value function in content/child/v8_value_converter_impl.cc in the V8 bindings in Google Chrome before 51.0.2704.63 does not properly restrict use of getters and setters, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code. **Reference:** CVE-2016-1679	http://googlechromereleases.blogspot.com/2016/05/stable-channel-update_25.html	A-GOO-CHROM-270616/72
DoS Overflow	2016-06-05	6.8	objects.cc in Google V8 before 5.0.71.32, as used in Google Chrome before 51.0.2704.63, does not properly restrict lazy deoptimization, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JavaScript code. **Reference:** CVE-2016-1678	http://googlechromereleases.blogspot.com/2016/05/stable-channel-update_25.html	A-GOO-CHROM-270616/73

Chrome;V8:

Google Chrome is a browser that combines a minimal design with sophisticated technology to make the web faster, safer, and easier. V8 is Google's open source high-performance JavaScript engine, written in C++ and used in Google Chrome, the open source browser from Google.

+Info	2016-06-05	4.3	uri.js in Google V8 before 5.1.281.26, as used in Google Chrome before 51.0.2704.63, uses an incorrect array type, which allows remote attackers to obtain sensitive information by calling the decodeURI function and leveraging "type confusion." **Reference:** CVE-2016-1677	https://crbug.com/602970	A-GOO-CHROM-270616/74
Bypass	2016-06-05	6.8	extensions/renderer/resources/binding.js in the extension bindings in Google Chrome before 51.0.2704.63 does not properly use prototypes, which allows remote attackers to bypass the Same Origin Policy via unspecified vectors. **Reference:** CVE-2016-1676	http://googlechromereleases.blogspot.com/2016/05/stable-channel-update_25.html	A-GOO-CHROM-270616/75
Bypass	2016-06-05	6.8	Blink, as used in Google Chrome before 51.0.2704.63, allows remote attackers to bypass the Same Origin Policy by leveraging the mishandling of Document reattachment during destruction, related to FrameLoader.cpp and LocalFrame.cpp. **Reference:** CVE-2016-1675	http://googlechromereleases.blogspot.com/2016/05/stable-channel-update_25.html	A-GOO-CHROM-270616/76
Bypass	2016-	6.8	The extensions subsystem in Google	https://crbug.com/5981	A-GOO-

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

	06-05		Chrome before 51.0.2704.63 allows remote attackers to bypass the Same Origin Policy via unspecified vectors. **Reference:** CVE-2016-1674	65	CHROM-270616/77
Bypass	2016-06-05	6.8	Blink, as used in Google Chrome before 51.0.2704.63, allows remote attackers to bypass the Same Origin Policy via unspecified vectors. **Reference:** CVE-2016-1673	https://crbug.com/597532	A-GOO-CHROM-270616/78
Bypass	2016-06-05	6.8	The ModuleSystem::RequireForJsInner function in extensions/renderer/module_system.cc in the extension bindings in Google Chrome before 51.0.2704.63 mishandles properties, which allows remote attackers to conduct bindings-interception attacks and bypass the Same Origin Policy via unspecified vectors. **Reference:** CVE-2016-1672	http://googlechromereleases.blogspot.com/2016/05/stable-channel-update_25.html	A-GOO-CHROM-270616/79
Application;OS					
IBM/Suse					
Java Sdk; Websphere Application Server/Linux Enterprise Server;Linux Enterprise Software Development Kit: The Java Development Kit is a collection of tools that developers use to deploy applications written in Java					
+Info	2016-06-06	6.4	The J9 JVM in IBM SDK, Java Technology Edition 6 before SR16 FP20, 6 R1 before SR8 FP20, 7 before SR9 FP30, and 7 R1 before SR3 FP30 allows remote attackers to obtain sensitive information or inject data by invoking non-public interface methods. **Reference:** CVE-2015-5041	http://www-01.ibm.com/support/docview.wss?uid=swg21974194	A-IBM-JAVA -270616/80
OS					
XEN					
XEN: XenServer is the leading open source virtualization platform, powered by the Xen hypervisor.					
DoS	2016-06-07	4.7	The p2m_teardown function in arch/arm/p2m.c in Xen 4.4.x through 4.6.x allows local guest OS users with access to the driver domain to cause a denial of service (NULL pointer dereference and host OS crash) by creating concurrent domains and holding references to them, related to VMID exhaustion. **Reference:** CVE-2016-5242	http://xenbits.xen.org/xsa/advisory-181.html	O-XEN-XEN-270616/81
DoS	2016-06-07	1.9	The libxl device-handling in Xen through 4.6.x allows local guest OS users with access to the driver domain to cause a denial of service (management tool confusion) by manipulating information in the backend directories in xenstore. **Reference:** CVE-2016-4963	http://xenbits.xen.org/xsa/advisory-178.html	O-XEN-XEN-270616/82
DoS +Priv	2016-06-07	6.8	The libxl device-handling in Xen 4.6.x and earlier allows local OS guest administrators to cause a	http://xenbits.xen.org/xsa/advisory	O-XEN-XEN-

CVE 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 (resource consumption or management facility confusion) or gain host OS privileges by manipulating information in guest controlled areas of xenstore. **Reference:** CVE-2016-4962	-175.html	270616/83
Application					
F5					
Big-ip Access Policy Manager;Big-ip Advanced Firewall Manager;Big-ip Analytics;Big-ip Application Acceleration Manager;Big-ip Application Security Manager;Big-ip Global Traffic Manager;Big-ip Link Controller;Big-ip Local Traffic Manager;Big-ip Policy Enforcement Manager: A central policy control point delivers access based on context and is critical to managing a scalable, secure, and dynamic environment. F5 BIG-IP®Access Policy Manager® (APM) is a flexible, high-performance access and security solution that provides unified global access to your applications, network, and cloud.					
DoS	2016-06-07	5	Virtual servers in F5 BIG-IP 11.5.4, when SSL profiles are enabled, allow remote attackers to cause a denial of service (resource consumption and Traffic Management Microkernel restart) via an SSL alert during the handshake. **Reference:** CVE-2016-4545	https://support.f5.com/kb/en-us/solutions/public/k/48/sol48042976.html	A-F5-BIG-I-270616/84
OS;Application					
Canonical;Debian/Nginx					
Ubuntu Linux/Debian Linux/Nginx: Ubuntu is an open source software platform. NGINX is one of a handful of servers written to address the C10K problem					
DOS	2016-06-07	5	os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file. **Reference:** CVE-2016-4450	NA	O-CAN-UBUNT-270616/85
Application					
Apache					
Shiro: Apache Shiro is a powerful and easy-to-use Java security framework that performs authentication, authorization, cryptography, and session management.					
Exec Code Bypass	2016-06-07	6.8	Apache Shiro before 1.2.5, when a cipher key has not been configured for the "remember me" feature, allows remote attackers to execute arbitrary code or bypass intended access restrictions via an unspecified request parameter. **Reference:** CVE-2016-4437	NA	A-APA-SHIRO-270616/86
Struts/Ognl: Apache Struts 1 is a discontinued open-source web application framework for developing Java EE web applications. OGNL stands for Object-Graph Navigation Language; it is an expression language for getting and setting properties of Java objects, plus other extras such as list projection and selection and lambda expressions.					
DoS	2016-06-07	5	Apache Struts 2.0.0 through 2.3.24.1 does not properly cache method references when used with OGNL before 3.0.12, which allows remote	http://struts.apache.org/docs/s2-034.html	A-APA-STRUT-

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

			attackers to cause a denial of service (block access to a web site) via unspecified vectors. **Reference:** CVE-2016-3093		270616/87
Exec Code	2016-06-07	7.5	Apache Struts 2.3.20.x before 2.3.20.3, 2.3.24.x before 2.3.24.3, and 2.3.28.x before 2.3.28.1, when Dynamic Method Invocation is enabled, allow remote attackers to execute arbitrary code via vectors related to an ! (exclamation mark) operator to the REST Plugin. **Reference:** CVE-2016-3087	http://struts.apache.org/docs/s2-033.html	A-APA-STRUT-270616/88
Katello;Redhat					
Katello/Satellite: Katello brings the full power of content management alongside the provisioning and configuration capabilities of Foreman.					
Exec Code Sql	2016-06-07	6.5	Multiple SQL injection vulnerabilities in the scoped_search function in app/controllers/katello/api/v2/api_controller.rb in Katello allow remote authenticated users to execute arbitrary SQL commands via the (1) sort_by or (2) sort_order parameter. **Reference:** CVE-2016-3072	https://github.com/Katello/katello/pull/6051	A-KAT-KATEL-270616/89
Application;OS					
7-zip/Novell					
7zip/Opensuse: openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.					
DoS Exec Code Overflow	2016-06-07	6.8	The CInArchive::ReadFileItem method in Archive/Udf/UdfIn.cpp in 7zip 9.20 and 15.05 beta allows remote attackers to cause a denial of service (out-of-bounds read) or execute arbitrary code via the PartitionRef field in the Long Allocation Descriptor in a UDF file. **Reference:** CVE-2016-2335	NA	A-7-Z-7ZIP/-270616/90
OS;Application					
Debian/Zend					
Debian Linux/Zend Framework: Zend Framework (ZF) is an open source, object-oriented web application framework implemented in PHP 5 and licensed under the New BSD License.					
Exec Code Sql	2016-06-07	7.5	The PDO adapters in Zend Framework before 1.12.16 do not filer null bytes in SQL statements, which allows remote attackers to execute arbitrary SQL commands via a crafted query. **Reference:** CVE-2015-7695	http://framework.zend.com/security/advisory/ZF2015-08	O-DEB-DEBIA-270616/91
Apache					
James Server: Apache James Server is a 100% pure JAVA capable Mail Server running on Java 1.5 onwards.					
Exec Code	2016-06-07	9.3	Apache James Server 2.3.2, when configured with file-based user repositories, allows attackers to	https://blogs.apache.org/james/entr	A-APA-JAMES-

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

			execute arbitrary system commands via unspecified vectors. **Reference:** CVE-2015-7611	y/apache_james_server_2_3	270616/92

OS;Application

Debian/Doctrine-project;Zend

Debian Linux/Annotations;Cache;Common;Doctrinemongodbbundle;Mongodb-odm;Object Relational Mapper/Zend Framework;Zend-cache;Zf-apigility-doctrine:
Debian is an operating system and a distribution of Free Software.

Exec Code	2016-06-07	7.2	Doctrine Annotations before 1.2.7, Cache before 1.3.2 and 1.4.x before 1.4.2, Common before 2.4.3 and 2.5.x before 2.5.1, ORM before 2.4.8 or 2.5.x before 2.5.1, MongoDB ODM before 1.0.2, and MongoDB ODM Bundle before 3.0.1 use world-writable permissions for cache directories, which allows local users to execute arbitrary PHP code with additional privileges by leveraging an application with the umask set to 0 and that executes cache entries as code. **Reference:** CVE-2015-5723	http://www.doctrine-project.org/2015/08/31/security_misconfiguration_vulnerability_in_various_doctrine_projects.html	O-DEB-DEBIA-270616/93

Canonical;Debian;Redhat/Spice Project

Ubuntu Linux/Debian Linux/Enterprise Linux Desktop;Enterprise Linux Hpc Node;Enterprise Linux Hpc Node Eus;Enterprise Linux Server;Enterprise Linux Server Eus;Enterprise Linux Workstation/Spice:
Ubuntu is an open source software platform. Linux is an operating system.

Overflow	2016-06-07	3.6	Heap-based buffer overflow in SPICE before 0.12.6 allows guest OS users to read and write to arbitrary memory locations on the host via guest QXL commands related to surface creation. **Reference:** CVE-2015-5261	https://bugzilla.redhat.com/show_bug.cgi?id=1261889	O-CAN-UBUNT-270616/94
DoS Exec Code Overflow Mem. Corr.	2016-06-07	7.2	Heap-based buffer overflow in SPICE before 0.12.6 allows guest OS users to cause a denial of service (heap-based memory corruption and QEMU-KVM crash) or possibly execute arbitrary code on the host via QXL commands related to the surface_id parameter. **Reference:** CVE-2015-5260	https://bugzilla.redhat.com/show_bug.cgi?id=1260822	O-CAN-UBUNT-270616/95

Criu/Novell

Criu/Opensuse: criu is a utility to checkpoint/restore a process tree. openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies

+Info	2016-06-07	2.1	The service daemon in CRIU does not properly restrict access to non-dumpable processes, which allows local users to obtain sensitive information via (1) process dumps or (2) ptrace access. **Reference:** CVE-2015-5231	https://bugzilla.redhat.com/show_bug.cgi?id=1256728	A-CRI-CRIU/-270616/96

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

NA	2016-06-07	7.2	The service daemon in CRIU creates log and dump files insecurely, which allows local users to create arbitrary files and take ownership of existing files via unspecified vectors related to a directory path. **Reference:** CVE-2015-5228	https://bugzilla.redhat.com/show_bug.cgi?id=1255782	A-CRI-CRIU/-270616/97
Debian/Freetype					
Debian Linux/Freetype: Debian is an operating system and a distribution of Free Software. FreeType is a popular software development library, used to render text on to bitmaps and provides support for other font-related operations					
DoS	2016-06-07	5	The t42_parse_encoding function in type42/t42parse.c in FreeType before 2.5.4 does not properly update the current position for immediates-only mode, which allows remote attackers to cause a denial of service (infinite loop) via a Type42 font. **Reference:** CVE-2014-9747	http://git.savannah.gnu.org/cgit/freetype/freetype2.git/tree/src/type42/t42parse.c?id=8b281f83e8516535756f92dbf90940ac44bd45e1	O-DEB-DEBIA-270616/98
DoS	2016-06-07	7.5	The (1) t1_parse_font_matrix function in type1/t1load.c, (2) cid_parse_font_matrix function in cid/cidload.c, (3) t42_parse_font_matrix function in type42/t42parse.c, and (4) ps_parser_load_field function in psaux/psobjs.c in FreeType before 2.5.4 do not check return values, which allows remote attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via a crafted font. **Reference:** CVE-2014-9746	http://git.savannah.gnu.org/cgit/freetype/freetype2.git/commit/?id=8b281f83e8516535756f92dbf90940ac44bd45e1	O-DEB-DEBIA-270616/99
Redhat					
Gluster Storage Management Console;Gluster Storage Server;Storage Native Client: Gluster Storage Platform offers an easy-to-use wizard-based system					
Bypass	2016-06-07	4	The Red Hat gluster-swift package, as used in Red Hat Gluster Storage (formerly Red Hat Storage Server), allows remote authenticated users to bypass the max_meta_count constraint via multiple crafted requests which exceed the limit when combined. **Reference:** CVE-2014-8177	https://bugzilla.redhat.com/show_bug.cgi?id=1257525	A-RED-GLUST-270616/100
Python					
Python: Python is a widely used high-level, general-purpose, interpreted, dynamic programming language.					
NA	2016-06-07	4.3	The ssl.match_hostname function in CPython (aka Python) before 2.7.9 and 3.x before 3.3.3 does not properly handle wildcards in hostnames, which might allow man-in-the-middle attackers to spoof servers via a crafted certificate. **Reference:** CVE-2013-7440	https://hg.python.org/cpython/rev/10d0edadbcdd	A-PYT-PYTHO-270616/101

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

OS;Application

Debian/Videolan

Debian Linux/Vlc Media Player:

Debian is an operating system and a distribution of Free Software.VLC is a free and open source cross-platform multimedia player and framework that plays most multimedia files as well as DVDs, Audio CDs, VCDs.

DoS Exec Code Overflow	2016-06-08	7.5	Buffer overflow in the DecodeAdpcmImaQT function in modules/codec/adpcm.c in VideoLAN VLC media player before 2.2.4 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted QuickTime IMA file. **Reference:** CVE-2016-5108	http://www.videolan.org/security/sa1601.html	O-DEB-DEBIA-270616/102

Application

HP

Discovery And Dependency Mapping Inventory:

Discovery and Dependency Mapping Inventory combines network discovery, hardware and software utilization to enable better utilization of IT assets.

Exec Code	2016-06-08	6.5	HPE Discovery and Dependency Mapping Inventory (DDMi) 9.30, 9.31, 9.32, 9.32 update 1, 9.32 update 2, and 9.32 update 3 allows remote authenticated users to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections library. **Reference:** CVE-2016-4369	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05164819	A-HP-DISCO-270616/103

Universal Cmbd Configuration Manager;Universal Cmbd Foundation;Universal Discovery:

The HPE Universal CMDB, a configuration management database solution, automatically collects and manages accurate and updated business service definitions, associated infrastructure relationships and detailed information on the assets, and is a central component in many of the key processes in your IT organization. HPE Universal Discovery (UD) software combines the automation of inventory discovery and dependency mapping.

Exec Code	2016-06-08	7.5	HPE Universal CMDB 10.0 through 10.21, Universal CMDB Configuration Manager 10.0 through 10.21, and Universal Discovery 10.0 through 10.21 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library. **Reference:** CVE-2016-4368	NA	A-HP-UNIVE-270616/104
+Info	2016-06-08	5	The Universal Discovery component in HPE Universal CMDB 10.0, 10.01, 10.10, 10.11, 10.20, and 10.21 allows remote attackers to obtain sensitive information via unspecified vectors. **Reference:** CVE-2016-4367	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05164813	A-HP-UNIVE-270616/105
DoS +Info	2016-06-08	7.5	HPE Systems Insight Manager (SIM) before 7.5.1 allows remote attackers to obtain sensitive information, modify data, or cause a denial of service via unspecified vectors. **Reference:** CVE-2016-4366	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05131085	A-HP-UNIVE-270616/106

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

+Info	2016-06-08	5	HPE Insight Control server deployment allows remote attackers to obtain sensitive information via unspecified vectors. **Reference:** CVE-2016-4365	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05150800	A-HP-UNIVE-270616/107
+Priv	2016-06-08	7.2	HPE Insight Control server deployment allows local users to gain privileges via unspecified vectors. **Reference:** CVE-2016-4364	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05150800	A-HP-UNIVE-270616/108
XSS	2016-06-08	4.3	HPE Insight Control server deployment allows remote attackers to modify data via unspecified vectors. **Reference:** CVE-2016-4363	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05150800	A-HP-UNIVE-270616/109
+Info	2016-06-08	5.5	HPE Insight Control server deployment allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors. **Reference:** CVE-2016-4362	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05150800	A-HP-UNIVE-270616/110
DoS	2016-06-08	5	HPE LoadRunner 11.52 through patch 3, 12.00 through patch 1, 12.01 through patch 3, 12.02 through patch 2, and 12.50 through patch 3 and Performance Center 11.52 through patch 3, 12.00 through patch 1, 12.01 through patch 3, 12.20 through patch 2, and 12.50 through patch 1 allow remote attackers to cause a denial of service via unspecified vectors. **Reference:** CVE-2016-4361	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05157423	A-HP-UNIVE-270616/111
	2016-06-08	6.4	The import_csv functionality in HPE LoadRunner 11.52 through patch 3, 12.00 through patch 1, 12.01 through patch 3, 12.02 through patch 2, and 12.50 through patch 3 and Performance Center 11.52 through patch 3, 12.00 through patch 1, 12.01 through patch 3, 12.20 through patch 2, and 12.50 through patch 1 do not restrict file paths sent to an unlink call, which allows remote attackers to delete arbitrary files via unspecified vectors, aka ZDI-CAN-3555. **Reference:** CVE-2016-4360	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05157423	A-HP-UNIVE-270616/112
	2016-06-08	7.5	Stack-based buffer overflow in mchan.dll in HPE LoadRunner 11.52 through patch 3, 12.00 through patch 1, 12.01 through patch 3, 12.02 through patch 2, and 12.50 through patch 3 and Performance Center 11.52 through patch 3, 12.00 through patch 1, 12.01 through patch 3, 12.20 through patch 2, and 12.50 through patch 1 allows remote attackers to execute arbitrary code via vectors related to constructing a shared memory file name, aka ZDI-CAN-3516. **Reference:** CVE-2016-4359	Exec Code Overflow https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05157423	A-HP-UNIVE-270616/113

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

+Info	2016-06-08	4.8	HPE Matrix Operating Environment before 7.5.1 allows remote attackers to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than CVE-2016-2029. **Reference:** CVE-2016-4358	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05150888	A-HP-UNIVE-270616/114
+Info	2016-06-08	7.5	HPE Matrix Operating Environment before 7.5.1 allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than CVE-2016-2028. **Reference:** CVE-2016-4357	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05150888	A-HP-UNIVE-270616/115
Redhat					
Openshift: 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. OpenShift Origin is an application platform where developers and teams can build, test, deploy, and run their applications.					
+Priv	2016-06-08	6.5	Red Hat OpenShift Enterprise 3.2 does not properly restrict access to STI builds, which allows remote authenticated users to access the Docker socket and gain privileges via vectors related to build-pod. **Reference:** CVE-2016-3738	https://access.redhat.com/errata/RHSA-2016:1094	A-RED-OPENS-270616/116
+Info	2016-06-08	2.1	HAproxy in Red Hat OpenShift Enterprise 3.2 and OpenShift Origin allows local users to obtain the internal IP address of a pod by reading the "OPENSHIFT_[namespace]_SERVERID" cookie. **Reference:** CVE-2016-3711	https://github.com/openshift/origin/pull/8334	A-RED-OPENS-270616/117
NA	2016-06-08	5.5	Red Hat OpenShift Enterprise 3.2, when multi-tenant SDN is enabled and a build is run in a namespace that would normally be isolated from pods in other namespaces, allows remote authenticated users to access network resources on restricted pods via an s2i build with a builder image that (1) contains ONBUILD commands or (2) does not contain a tar binary. **Reference:** CVE-2016-3708	https://access.redhat.com/errata/RHSA-2016:1094	A-RED-OPENS-270616/118
NA	2016-06-08	3.5	Red Hat OpenShift Enterprise 3.2 and 3.1 do not properly validate the origin of a request when anonymous access is granted to a service/proxy or pod/proxy API for a specific pod, which allows remote attackers to access API credentials in the web browser localStorage via an access_token in the query parameter. **Reference:** CVE-2016-3703	NA	A-RED-OPENS-270616/119
Exec Code	2016-06-08	9	Red Hat OpenShift Enterprise 3.2 and OpenShift Origin allow remote authenticated users to execute commands with root privileges by changing the root password in an sti builder image. **Reference:** CVE-2016-2160	https://bugzilla.redhat.com/show_bug.cgi?id=1316127	A-RED-OPENS-270616/120

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

+Info	2016-06-08	4	Red Hat OpenShift Enterprise 3.2 allows remote authenticated users to read log files from another namespace by using the same name as a previously deleted namespace when creating a new namespace. **Reference:** CVE-2016-2149	https://access.redhat.com/errata/RHSA-2016:1064	A-RED-OPENS-270616/121
+Info	2016-06-08	2.1	Red Hat OpenShift Enterprise 3.1 uses world-readable permissions on the /etc/origin/master/master-config.yaml configuration file, which allows local users to obtain Active Directory credentials by reading the file. **Reference:** CVE-2016-2142	https://access.redhat.com/errata/RHSA-2016:1038	A-RED-OPENS-270616/122
Vmware					
Vcenter Server: vCenter server is installed on Windows Server 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.					
XSS	2016-06-08	4.3	Cross-site scripting (XSS) vulnerability in the Web Client in VMware vCenter Server 5.1 before update 3d, 5.5 before update 3d, and 6.0 before update 2 on Windows allows remote attackers to inject arbitrary web script or HTML via the flashvars parameter. **Reference:** CVE-2016-2078	http://www.vmware.com/security/advisories/VMSA-2016-0006.html	A-VMW-VCENT-270616/123
HP					
Systems Insight Manager: HPE Systems Insight Manager (HPE SIM) is the foundation for the HPE unified server-storage management strategy.					
+Info	2016-06-08	5.5	HPE Systems Insight Manager (SIM) before 7.5.1 allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than CVE-2016-2017, CVE-2016-2019, CVE-2016-2020, CVE-2016-2021, and CVE-2016-2022. **Reference:** CVE-2016-2030	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05131085	A-HP-SYSTE-270616/124
Matrix Operating Environment;Systems Insight Manager: Matrix Operating Environment integrates all of the virtualized components to enable on-demand fulfillment of server, storage, and networking functions to meet the business computing needs. HPE Systems Insight Manager (HPE SIM) is the foundation for the HPE unified server-storage management strategy.					
+Info	2016-06-08	6.4	HPE Matrix Operating Environment before 7.5.1 allows remote attackers to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than CVE-2016-4358. **Reference:** CVE-2016-2029	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05150888	A-HP-MATRI-270616/125
+Info	2016-06-08	5.5	HPE Matrix Operating Environment before 7.5.1 allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than CVE-2016-4357. **Reference:** CVE-2016-2028	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05150888	A-HP-MATRI-270616/126
+Info	2016-06-08	5	HPE Matrix Operating Environment before 7.5.1 allows remote attackers to obtain sensitive	https://h20566.www2.hpe.com/por	A-HP-MATRI-

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

			information via unspecified vectors, a different vulnerability than CVE-2016-2026. **Reference:** CVE-2016-2027	tal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05150888	270616/127
+Info	2016-06-08	5	HPE Matrix Operating Environment before 7.5.1 allows remote attackers to obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2016-2027. **Reference:** CVE-2016-2026	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05150888	A-HP-MATRI-270616/128
Insight Contol: Insight Control server provisioning uses resources such as OS Build Plans and scripts to rundeployment jobs.					
DoS +Info	2016-06-08	7.5	HPE Insight Control before 7.5.1 allow remote attackers to obtain sensitive information, modify data, or cause a denial of service via unspecified vectors. **Reference:** CVE-2016-2024	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05158380	A-HP-INSIG-270616/129
Systems Insight Manager: HPE Systems Insight Manager (HPE SIM) is the foundation for the HPE unified server-storage management strategy.					
+Info	2016-06-08	4.7	HPE Systems Insight Manager (SIM) before 7.5.1 allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than CVE-2016-2017, CVE-2016-2019, CVE-2016-2020, CVE-2016-2021, and CVE-2016-2030. **Reference:** CVE-2016-2022	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05131085	A-HP-SYSTE-270616/130
+Info	2016-06-08	7.7	HPE Systems Insight Manager (SIM) before 7.5.1 allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than CVE-2016-2017, CVE-2016-2019, CVE-2016-2020, CVE-2016-2022, and CVE-2016-2030. **Reference:** CVE-2016-2021	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05131085	A-HP-SYSTE-270616/131
+Info	2016-06-08	8.5	HPE Systems Insight Manager (SIM) before 7.5.1 allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than CVE-2016-2017, CVE-2016-2019, CVE-2016-2021, CVE-2016-2022, and CVE-2016-2030. **Reference:** CVE-2016-2020	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05131085	A-HP-SYSTE-270616/132
+Info	2016-06-08	7.7	HPE Systems Insight Manager (SIM) before 7.5.1 allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than CVE-2016-2017, CVE-2016-2020, CVE-2016-2021, CVE-2016-2022, and CVE-2016-2030. **Reference:** CVE-2016-2019	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05131085	A-HP-SYSTE-270616/133
+Info	2016-06-08	6.4	HPE Systems Insight Manager (SIM) before 7.5.1 allows remote attackers to obtain sensitive information or modify data via unspecified vectors. **Reference:** CVE-2016-2018	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05131085	A-HP-SYSTE-270616/134
+Info	2016-	5.5	HPE Systems Insight Manager (SIM) before 7.5.1	https://h20566.w	A-HP-

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

	06-08		allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than CVE-2016-2019, CVE-2016-2020, CVE-2016-2021, CVE-2016-2022, and CVE-2016-2030. **Reference:** CVE-2016-2017	ww2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05131085	SYSTE-270616/135
Cisco					
Aironet Access Point Software: Cisco Aironet IP setup utility used to configure IP addresses of all Aironet Access Points, Wireless Bridges and Workgroup Bridges.					
NA	2016-06-08	7.2	Cisco Aironet Access Point Software 8.2(100.0) on 1830e, 1830i, 1850e, 1850i, 2800, and 3800 access points allows local users to obtain Linux root access via crafted CLI command parameters, aka Bug ID CSCuy64037. **Reference:** CVE-2016-1418	NA	A-CIS-AIRON-270616/136
Cisco;Clamav					
Email Security Appliance;Web Security Appliance/Clamav: Cisco Email Security Appliances defend mission-critical email systems at the gateway, and automatically stop spam, viruses, and other threats.Clam AntiVirus (ClamAV) is a free and open-source, cross-platform antivirus software toolkit able to detect many types of malicious software, including viruses.					
DoS Overflow	2016-06-08	5	libclamav in ClamAV (aka Clam AntiVirus), as used in Advanced Malware Protection (AMP) on Cisco Email Security Appliance (ESA) devices before 9.7.0-125 and Web Security Appliance (WSA) devices before 9.0.1-135 and 9.1.x before 9.1.1-041, allows remote attackers to cause a denial of service (AMP process restart) via a crafted document, aka Bug IDs CSCuv78533 and CSCuw60503. **Reference:** CVE-2016-1405	NA	A-CIS-EMAIL-270616/137
Application;OS					
Symantec/Symantec					
Critical System Protection;Data Center Security Server;Data Center Security Serverand Agents/Symantec Embedded Security Critical System Protection;Symantec Embedded Security Critical System Protection For Controllers And Devices: The Symantec Critical System Protection (SCSP) is a solution offered by the Symantec data center Security team to protect servers in data centers. S ymantec Data Center Security- Server Advanced (SDCS: SA) provides a policy-based approach to endpoint security and compliance.					
NA	2016-06-08	4.9	Symantec Embedded Security: Critical System Protection (SES:CSP) 1.0.x before 1.0 MP5, Embedded Security: Critical System Protection for Controllers and Devices (SES:CSP) 6.5.0 before MP1, Critical System Protection (SCSP) before 5.2.9 MP6, Data Center Security: Server Advanced Server (DCS:SA) 6.x before 6.5 MP1 and 6.6 before MP1, and Data Center Security: Server Advanced Server and Agents (DCS:SA) through 6.6 MP1 allow remote authenticated users to conduct argument-injection attacks by leveraging certain named-pipe access. **Reference:** CVE-2015-8800	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160607_00	A-SYM-CRITI-270616/138

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

Dir. Trav.	2016-06-08	7.1	Directory traversal vulnerability in the Management Server in Symantec Embedded Security: Critical System Protection (SES:CSP) 1.0.x before 1.0 MP5, Embedded Security: Critical System Protection for Controllers and Devices (SES:CSP) 6.5.0 before MP1, Critical System Protection (SCSP) before 5.2.9 MP6, Data Center Security: Server Advanced Server (DCS:SA) 6.x before 6.5 MP1 and 6.6 before MP1, and Data Center Security: Server Advanced Server and Agents (DCS:SA) through 6.6 MP1 allows remote authenticated users to write update-package data to arbitrary agent locations via unspecified vectors. **Reference:** CVE-2015-8799	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160607_00	A-SYM-CRITI-270616/139
Exec Code Dir. Trav.	2016-06-08	7.7	Directory traversal vulnerability in the Management Server in Symantec Embedded Security: Critical System Protection (SES:CSP) 1.0.x before 1.0 MP5, Embedded Security: Critical System Protection for Controllers and Devices (SES:CSP) 6.5.0 before MP1, Critical System Protection (SCSP) before 5.2.9 MP6, Data Center Security: Server Advanced Server (DCS:SA) 6.x before 6.5 MP1 and 6.6 before MP1, and Data Center Security: Server Advanced Server and Agents (DCS:SA) through 6.6 MP1 allows remote authenticated users to execute arbitrary code via unspecified vectors. **Reference:** CVE-2015-8798	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160607_00	A-SYM-CRITI-270616/140
Exec Code Sql	2016-06-08	6.5	SQL injection vulnerability in the Management Server in Symantec Embedded Security: Critical System Protection (SES:CSP) 1.0.x before 1.0 MP5, Embedded Security: Critical System Protection for Controllers and Devices (SES:CSP) 6.5.0 before MP1, Critical System Protection (SCSP) before 5.2.9 MP6, Data Center Security: Server Advanced Server (DCS:SA) 6.x before 6.5 MP1 and 6.6 before MP1, and Data Center Security: Server Advanced Server and Agents (DCS:SA) through 6.6 MP1 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors. **Reference:** CVE-2015-8157	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160607_00	A-SYM-CRITI-270616/141
Vtscada					
Vtscada: VTScada HMI SCADA software allows system integrators, OEMs or end users to develop PC-based industrial monitoring & control applications.					
Dir. Trav.	2016-06-09	6.4	Directory traversal vulnerability in the WAP interface in Trihedral VTScada (formerly VTS) 8.x through 11.x before 11.2.02 allows remote attackers to read arbitrary files via a crafted pathname. **Reference:** CVE-2016-4532	https://ics-cert.us-cert.gov/advisories/ICSA-16-159-01	A-TRI-VTSCA-270616/142
ABB					
Pcm600: The Protection and Control IED Manager PCM600 tool provides versatile functionalities for the entire life-cycle of all Relion® protection and control IED applications, at all voltage levels.					

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

+Info	2016-06-09	1.9	ABB PCM600 before 2.7 improperly stores PCM600 authentication credentials, which allows local users to obtain sensitive information via unspecified vectors. **Reference:** CVE-2016-4527	https://ics-cert.us-cert.gov/advisories/ICSA-16-152-02	A-ABB-PCM60-270616/143
+Info	2016-06-09	2.1	ABB PCM600 before 2.7 improperly stores OPC Server IEC61850 passwords in unspecified temporary circumstances, which allows local users to obtain sensitive information via unknown vectors. **Reference:** CVE-2016-4524	https://ics-cert.us-cert.gov/advisories/ICSA-16-152-02	A-ABB-PCM60-270616/144
Trihedral					
Vtscada: VTScada HMI SCADA software allows system integrators, OEMs or end users to develop PC-based industrial monitoring & control applications.					
DoS Overflow	2016-06-09	5	The WAP interface in Trihedral VTScada (formerly VTS) 8.x through 11.x before 11.2.02 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via unspecified vectors. **Reference:** CVE-2016-4523	https://ics-cert.us-cert.gov/advisories/ICSA-16-159-01	A-TRI-VTSCA-270616/145
ABB					
Pcm600: The Protection and Control IED Manager PCM600 tool provides versatile functionalities for the entire life-cycle of all Relion® protection and control IED applications, at all voltage levels.					
+Info	2016-06-09	2.1	ABB PCM600 before 2.7 improperly stores the main application password after a password change, which allows local users to obtain sensitive information via unspecified vectors. **Reference:** CVE-2016-4516	https://ics-cert.us-cert.gov/advisories/ICSA-16-152-02	A-ABB-PCM60-270616/146
+Info	2016-06-09	0	ABB PCM600 before 2.7 uses an improper hash algorithm for the main application password, which makes it easier for local users to obtain sensitive cleartext information by leveraging read access to the ACTConfig configuration file. **Reference:** CVE-2016-4511	https://ics-cert.us-cert.gov/advisories/ICSA-16-152-02	A-ABB-PCM60-270616/147
Trihedral					
Vtscada: VTScada HMI SCADA software allows system integrators, OEMs or end users to develop PC-based industrial monitoring & control applications.					
Bypass	2016-06-09	6.4	The WAP interface in Trihedral VTScada (formerly VTS) 8.x through 11.x before 11.2.02 allows remote attackers to bypass authentication and read arbitrary files via unspecified vectors. **Reference:** CVE-2016-4510	https://ics-cert.us-cert.gov/advisories/ICSA-16-159-01	A-TRI-VTSCA-270616/148
OS					
Kmc Controls					
Bac-5051e Firmware: KMC Controls BAC-5051E Devices With Firmware Before E0.2.0.2 Allow Remote Attackers To Bypass Intended Access Restrictions					

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

Bypass	2016-06-09	5	KMC Controls BAC-5051E devices with firmware before E0.2.0.2 allow remote attackers to bypass intended access restrictions and read a configuration file via unspecified vectors. **Reference:** CVE-2016-4495	https://ics-cert.us-cert.gov/advisories/ICSA-16-126-01	O-KMC-BAC-5-270616/149
CSRF	2016-06-09	6.8	Cross-site request forgery (CSRF) vulnerability on KMC Controls BAC-5051E devices with firmware before E0.2.0.2 allows remote attackers to hijack the authentication of unspecified victims for requests that disclose the contents of a configuration file. **Reference:** CVE-2016-4494	https://ics-cert.us-cert.gov/advisories/ICSA-16-126-01	O-KMC-BAC-5-270616/150
OS;Application					
Canonical;Debian/Xmlsoft					
Ubuntu Linux/Debian Linux/Libxml2: Linux is a Unix-like and mostly POSIX-compliant computer operating system (OS) assembled under the model of free and open-source software development and distribution.libxml2 is a software library for parsing XML documents					
DoS	2016-06-09	5.8	XML external entity (XXE) vulnerability in the xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.4, when not in validating mode, allows context-dependent attackers to read arbitrary files or cause a denial of service (resource consumption) via unspecified vectors. **Reference:** CVE-2016-4449	https://git.gnome.org/browse/libxml2/commit/?id=b1d34de46a11323fccffa9fadeb33be670d602f5	O-CAN-UBUNT-270616/151
Application					
Xmlsoft					
Libxml2: libxml2 is a software library for parsing XML documents					
NA	2016-06-09	10	Format string vulnerability in libxml2 before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors. **Reference:** CVE-2016-4448	http://xmlsoft.org/news.html	A-XML-LIBXM-270616/152
OS;Application					
Canonical;Debian/Xmlsoft					
Ubuntu Linux/Debian Linux/Libxml2: Linux is a Unix-like and mostly POSIX-compliant computer operating system (OS) assembled under the model of free and open-source software development and distribution.libxml2 is a software library for parsing XML documents					
DoS Overflow	2016-06-09	5	The xmlParseElementDecl function in parser.c in libxml2 before 2.9.4 allows context-dependent attackers to cause a denial of service (heap-based buffer underread and application crash) via a crafted file, involving xmlParseName. **Reference:** CVE-2016-4447	https://git.gnome.org/browse/libxml2/commit/?id=00906759053986b8079985644172085f74331f83	O-CAN-UBUNT-270616/153

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

Application

HP

Project And Portfolio Management Center:

HP Project and Portfolio Management (PPM) Center standardizes, manages, and captures the execution of project and operational activities.

Exec Code +Info	2016-06-09	6.5	HPE Project and Portfolio Management Center (PPM) 9.2x and 9.3x before 9.32.0002 allows remote authenticated users to execute arbitrary commands or obtain sensitive information via unspecified vectors. **Reference:** CVE-2016-4370	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05167126	A-HP-PROJE-270616/154

Medhost

Perioperative Information Management System:

MEDHOST PIMS delivers real-time access to patient data and clinical systems.

+Info	2016-06-09	10	MEDHOST Perioperative Information Management System (aka PIMS or VPIMS) before 2015R1 has hardcoded credentials, which makes it easier for remote attackers to obtain sensitive information via direct requests to the application database server. **Reference:** CVE-2016-4328	http://www.kb.cert.org/vuls/id/482135	A-MED-PERIO-270616/155

Chef

Chef Manage:

The Chef management console enables the management of nodes, data bags, roles, environments, and cookbooks by using a web user interface.

Exec Code	2016-06-09	7.5	The Chef Manage (formerly opscode-manage) add-on before 1.12.0 for Chef allows remote attackers to execute arbitrary code via crafted serialized data in a cookie. **Reference:** CVE-2016-4326	http://www.kb.cert.org/vuls/id/586503	A-CHE-CHEF -270616/156

GE

Multilink Firmware:

P&E's USB Multilink Universal is an all-in-one development interface which allows a PC access to the Background Debug Mode (BDM) or JTAG interface

NA	2016-06-09	10	General Electric (GE) Multilink ML800, ML1200, ML1600, and ML2400 switches with firmware before 5.5.0 and ML810, ML3000, and ML3100 switches with firmware before 5.5.0k have hardcoded credentials, which allows remote attackers to modify configuration settings via the web interface. **Reference:** CVE-2016-2310	https://ics-cert.us-cert.gov/advisories/ICSA-16-154-01	O-GE-MULTI-270616/157

OS;Application

Debian;Redhat/Spice Project

Debian Linux/Enterprise Linux;Enterprise Linux Desktop;Enterprise Linux Hpc Node Eus;Enterprise Linux Server;Enterprise Linux Server Aus;Enterprise Linux Server Eus;Enterprise Linux Workstation/Spice:

A Linux server is a high-powered variant of the Linux open source operating system that's designed to handle the more

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

demanding needs of business applications such as network and system administration, database management and Web services.					
NA	2016-06-09	3.6	SPICE allows local guest OS users to read from or write to arbitrary host memory locations via crafted primary surface parameters, a similar issue to CVE-2015-5261. **Reference:** CVE-2016-2150	https://bugzilla.redhat.com/show_bug.cgi?id=1313496	O-DEB-DEBIA-270616/158
Application;OS					
Canonical/Canonical					
LXD/Ubuntu Linux: LXD is a container "hypervisor" and a new user experience for LXC. Ubuntu is an open source software platform					
Info	2016-06-09	2.1	LXD before 2.0.2 does not properly set permissions when switching an unprivileged container into privileged mode, which allows local users to access arbitrary world readable paths in the container directory via unspecified vectors. **Reference:** CVE-2016-1582	https://linuxcontainers.org/lxd/news/+	A-CAN-LXD/U-270616/159
NA	2016-06-09	2.1	LXD before 2.0.2 uses world-readable permissions for /var/lib/lxd/zfs.img when setting up a loop based ZFS pool, which allows local users to copy and read data from arbitrary containers via unspecified vectors. **Reference:** CVE-2016-1581	https://linuxcontainers.org/lxd/news/	A-CAN-LXD/U-270616/160
OS					
Cisco					
Ip Phone 8800 Series Firmware: The Cisco IP Phone 8800 Series delivers HD video and VoIP communications, and integrates with your mobile device to meet your business needs.					
DoS Overflow	2016-06-09	5	The web application on Cisco IP 8800 devices allows remote attackers to cause a denial of service (out-of-bounds memory access and web-server outage) via a crafted request, aka Bug ID CSCuz03034. **Reference:** CVE-2016-1421	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160609-ipp	O-CIS-IP PH-270616/161
Hardware;OS					
Cisco/Cisco					
Application Infrastructure Controller/Application Policy Infrastructure Controller Firmware: The Cisco Application Policy Infrastructure Controller (Cisco APIC) is the unifying point of automation and management for the Application Centric Infrastructure (ACI) fabric.					
NA	2016-06-09	7.2	The installation component on Cisco Application Policy Infrastructure Controller (APIC) devices with software before 1.3(2f) mishandles binary files, which allows local users to obtain root access via unspecified vectors, aka Bug ID CSCuz72347. **Reference:** CVE-2016-1420	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160609-apic	H-CIS-APPLI-270616/162

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

OS					
Cisco					
Aironet Access Point Software: Cisco Aironet IP setup utility used to configure IP addresses of all Aironet Access Points, Wireless Bridges and Workgroup Bridges.					
DoS	2016-06-09	6.8	Cisco Access Point devices with software 8.2(102.43) allow remote attackers to cause a denial of service (device reload) via crafted ARP packets, aka Bug ID CSCuy55803. **Reference:** CVE-2016-1419	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160608-aironet	O-CIS-AIRON-270616/163
Application					
EMC					
Networker: EMC NetWorker (formerly Legato NetWorker) is a suite of enterprise level data protection software that unifies and automates backup to tape, disk-based, and flash-based storage media across physical and virtual environments for granular and disaster recovery.					
Exec Code	2016-06-09	10	EMC NetWorker 8.2.1.x and 8.2.2.x before 8.2.2.6 and 9.x before 9.0.0.6 mishandles authentication, which allows remote attackers to execute arbitrary commands by leveraging access to a different NetWorker instance. **Reference:** CVE-2016-0916	http://seclists.org/bugtraq/2016/Jun/43	A-EMC-NETWO-270616/164
OS					
EMC					
Data Domain Os: The EMC Data Domain Operating System delivers industry-leading speed and efficiency through variable-length deduplication.					
NA	2016-06-09	4.3	EMC Data Domain OS 5.5 before 5.5.4.0, 5.6 before 5.6.1.004, and 5.7 before 5.7.2.0 stores session identifiers of GUI users in a world-readable file, which allows local users to hijack arbitrary accounts via unspecified vectors. **Reference:** CVE-2016-0910	http://seclists.org/bugtraq/2016/Jun/44	O-EMC-DATA -270616/165
OS;Application					
Debian;Redhat/Spice Project					
Debian Linux/Enterprise Linux;Enterprise Linux Desktop;Enterprise Linux Hpc Node Eus;Enterprise Linux Server;Enterprise Linux Server Aus;Enterprise Linux Server Eus;Enterprise Linux Workstation/Spice: A Linux server is a high-powered variant of the Linux open source operating system that's designed to handle the more demanding needs of business applications such as network and system administration, database management and					
DoS Exec Code Overflow	2016-06-09	10	The smartcard interaction in SPICE allows remote attackers to cause a denial of service (QEMU-KVM process crash) or possibly execute arbitrary code via vectors related to connecting to a guest VM, which triggers a heap-based buffer overflow. **Reference:** CVE-2016-0749	NA	O-DEB-DEBIA-270616/166

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

Application					
Idera					
Uptime Infrastructure Monitor: Uptime Infrastructure Monitor offers integrated capacitymonitoring and reporting across multiple platforms, including Windows, Linux, UNIX, Novell, Virtual Servers (VMware, Hyper-V, Xen), Cloud, and more.					
+Info	2016-06-09	5	The up.time agent in Idera Uptime Infrastructure Monitor 7.5 and 7.6 on Linux allows remote attackers to read arbitrary files via unspecified vectors. **Reference:** CVE-2015-8268	http://jira.uptimesoftware.com/browse/UT-16039	A-IDE-UPTIM-270616/167
OS					
Huawei					
Mate 8 Firmware: Huawei Mate 8 is a very stylish smartphone from Huawei with large 6 inch display and Kirin 950 CPU.					
+Info	2016-06-10	4.3	Huawei Mate 8 smartphones with software NXT-AL10 before NXT-AL10C00B182, NXT-CL00 before NXT-CL00C92B182, NXT-DL00 before NXT-DL00C17B182, and NXT-TL00 before NXT-TL00C01B182 allow remote base stations to obtain sensitive subscriber signal strength information via vectors involving improper security status verification, aka HWPSIRT-2015-12007. **Reference:** CVE-2016-5233	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160520-03-smartphone-en	O-HUA-MATE -270616/168
OS;Application					
Debian;Novell/Graphicsmagick					
Debian Linux/Leap;Opensuse/Graphicsmagick: A Linux server is a high-powered variant of the Linux open source operating system that's designed to handle the more demanding needs of business applications such as network and system administration, database management and Web services.GraphicsMagick is a robust collection of tools and libraries to read, write, and manipulate an image in any of the more popular image formats including GIF. openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies					
Exec Code	2016-06-10	10	The OpenBlob function in blob.c in GraphicsMagick before 1.3.24 and ImageMagick allows remote attackers to execute arbitrary code via a | (pipe) character at the start of a filename. **Reference:** CVE-2016-5118	http://hg.code.sf.net/p/graphicsmagick/code/file/41876934e762/ChangeLog	O-DEB-DEBIA-270616/169
GNU/Novell					
Glibc/Opensuse: The GNU C Library, commonly known as glibc, is the GNU Project's implementation of the C standard library. Despite its name, it now also directly supports C++ (and, indirectly, other programming languages).					
DoS Overflow	2016-06-10	7.5	Stack-based buffer overflow in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or libc6) allows remote servers	https://sourceware.org/git/gitweb.cgi?p=glibc.git;h=	A-GNU-GLIBC-

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

			to cause a denial of service (crash) or possibly unspecified other impact via a flood of crafted ICMP and UDP packets. **Reference:** CVE-2016-4429	bc779a1a5b3035133024b21e2f339fe4219fb11c	270616/170

Fasterxml/Fedoraproject

Jackson/Fedora:

Jackson system development (JSD) is a linear software development methodology developed by Michael A. Jackson and John Cameron in the 1980s. Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project

NA	2016-06-10	10	XML external entity (XXE) vulnerability in XmlMapper in the Data format extension for Jackson (aka jackson-dataformat-xml) allows attackers to have unspecified impact via unknown vectors. **Reference:** CVE-2016-3720	http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184561.html	A-FAS-JACKS-270616/171

GNU/Novell

Glibc/Opensuse:

The GNU C Library, commonly known as glibc, is the GNU Project's implementation of the C standard library. Despite its name, it now also directly supports C++ (and, indirectly, other programming languages).

DoS Overflow	2016-06-10	5	Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in the GNU C Library (aka glibc or libc6) allows remote attackers to cause a denial of service (crash) via vectors involving hostent conversion. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-4458. **Reference:** CVE-2016-3706	https://sourceware.org/git/gitweb.cgi?p=glibc.git;h=4ab2ab03d4351914ee53248dc5aef4a8c88ff8b9	A-GNU-GLIBC-270616/172

Apache

Cloudstack:

CloudStack is open source cloud computing software for creating, managing, and deploying infrastructure cloud services.

Bypass	2016-06-10	5.8	Apache CloudStack 4.5.x before 4.5.2.1, 4.6.x before 4.6.2.1, 4.7.x before 4.7.1.1, and 4.8.x before 4.8.0.1, when SAML-based authentication is enabled and used, allow remote attackers to bypass authentication and access the user interface via vectors related to the SAML plugin. **Reference:** CVE-2016-3085	NA	A-APA-CLOUD-270616/173

Puppetlabs

Puppet Agent;Puppet Enterprise:

Puppet agent is the application that manages configurations on nodes. Puppet master is a Ruby application that compiles configurations for any number of Puppet agent nodes, using Puppet code and various other data sources.

Exec Code	2016-06-10	7.5	The pxp-agent component in Puppet Enterprise 2015.3.x before 2015.3.3 and Puppet Agent 1.3.x before 1.3.6 does not properly validate server certificates, which might allow remote attackers to spoof brokers and execute arbitrary commands via a crafted certificate. **Reference:** CVE-2016-2786	https://puppet.com/security/cve/CVE-2016-2786	A-PUP-PUPPE-270616/174
Bypass	2016-06-10	7.5	Puppet Server before 2.3.2 and Ruby puppetmaster in Puppet 4.x before 4.4.2 and in Puppet Agent before 1.4.2 might allow remote	https://github.com/puppetlabs/puppet/pull/4921/c	A-PUP-PUPPE-

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

			attackers to bypass intended auth.conf access restrictions by leveraging incorrect URL decoding. **Reference:** CVE-2016-2785	ommits/8d2ce797db265720f0a20d1d46ee2757b4e4f6b2	270616/175
OS					
Google					
Android: Android is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices					
+Info	2016-06-12	4.3	Activity Manager in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-06-01 does not properly terminate process groups, which allows attackers to obtain sensitive information via a crafted application, aka internal bug 19285814. **Reference:** CVE-2016-2500	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/176
+Info	2016-06-12	4.3	AudioSource.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 2016-06-01 does not initialize certain data, which allows attackers to obtain sensitive information via a crafted application, aka internal bug 27855172. **Reference:** CVE-2016-2499	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/177
Bypass +Info	2016-06-12	4.3	The Qualcomm Wi-Fi driver in Android before 2016-06-01 on Nexus 7 (2013) devices allows attackers to bypass intended data-access restrictions via a crafted application, aka internal bug 27777162. **Reference:** CVE-2016-2498	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/178
NA	2016-06-12	10	The Framework UI permission-dialog implementation in Android 6.x before 2016-06-01 allows attackers to conduct tapjacking attacks and access arbitrary private-storage files by creating a partially overlapping window, aka internal bug 26677796. **Reference:** CVE-2016-2496	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/179
DoS	2016-06-12	7.1	SampleTable.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 2016-06-01 allows remote attackers to cause a denial of service (device hang or reboot) via a crafted file, aka internal bug 28076789. **Reference:** CVE-2016-2495	https://android.googlesource.com/platform/frameworks/av/+/b57b3967b1a42dd505dbe4fcf1e1d810e3ae3777	O-GOO-ANDRO-270616/180
+Priv	2016-06-12	9.3	Off-by-one error in sdcard/sdcard.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 2016-06-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 28085658. **Reference:** CVE-2016-2494	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/181
+Priv	2016-06-12	9.3	The Broadcom Wi-Fi driver in Android before 2016-06-01 on Nexus 5, Nexus 6, Nexus 6P, Nexus 7 (2013), Nexus Player, and Pixel C devices allows attackers to gain privileges via a crafted	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/

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

			application, aka internal bug 26571522. **Reference:** CVE-2016-2493		182
+Priv	2016-06-12	0	The MediaTek power-management driver in Android before 2016-06-01 on Android One devices allows attackers to gain privileges via a crafted application, aka internal bug 28085410. **Reference:** CVE-2016-2492	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/183
+Priv	2016-06-12	9.3	The NVIDIA camera driver in Android before 2016-06-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27556408. **Reference:** CVE-2016-2491	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/184
+Priv	2016-06-12	9.3	The NVIDIA camera driver in Android before 2016-06-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27533373. **Reference:** CVE-2016-2490	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/185
+Priv	2016-06-12	9.3	The Qualcomm video driver in Android before 2016-06-01 on Nexus 5, 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 27407629. **Reference:** CVE-2016-2489	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/186
+Priv	2016-06-12	9.3	The Qualcomm camera driver in Android before 2016-06-01 on Nexus 5, 5X, 6, 6P, and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka internal bug 27600832. **Reference:** CVE-2016-2488	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/187
+Priv	2016-06-12	9.3	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 2016-06-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27833616. **Reference:** CVE-2016-2487	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/188
+Priv	2016-06-12	9.3	mp3dec/SoftMP3.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 2016-06-01 does not validate the relationship between allocated memory and the frame size, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27793371. **Reference:** CVE-2016-2486	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/189
Overflow +Priv	2016-06-12	9.3	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 2016-06-01 does not validate OMX buffer sizes for the GSM and G711 codecs, which	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/

CVE 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 gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27793367. **Reference:** CVE-2016-2485		190
Overflow +Priv	2016-06-12	9.3	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 2016-06-01 does not validate OMX buffer sizes for the GSM and G711 codecs, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27793163. **Reference:** CVE-2016-2484	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/191
Overflow +Priv	2016-06-12	9.3	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 2016-06-01 mishandles a buffer count, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27662502. **Reference:** CVE-2016-2483	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/192
Overflow +Priv	2016-06-12	9.3	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 2016-06-01 mishandles a buffer count, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27661749. **Reference:** CVE-2016-2482	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/193
Overflow +Priv	2016-06-12	9.3	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 2016-06-01 mishandles a buffer count, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27532497. **Reference:** CVE-2016-2481	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/194
+Priv	2016-06-12	9.3	The mm-video-v4l2 vidc 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 2016-06-01 does not validate certain OMX parameter data structures, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27532721. **Reference:** CVE-2016-2480	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/195
Overflow +Priv	2016-06-12	9.3	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 2016-06-01 mishandles a buffer count, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/196

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

			Signature or SignatureOrSystem access, aka internal bug 27532282. **Reference:** CVE-2016-2479		
+Priv	2016-06-12	9.3	mm-video-v4l2/vidc/vdec/src/omx_vdec_msm8974.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 2016-06-01 mishandles pointers, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27475409. **Reference:** CVE-2016-2478	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/197
+Priv	2016-06-12	9.3	mm-video-v4l2/vidc/vdec/src/omx_vdec_msm8974.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 2016-06-01 mishandles pointers, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27251096. **Reference:** CVE-2016-2477	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/198
Overflow +Priv	2016-06-12	9.3	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 2016-06-01 does not validate OMX buffer sizes, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27207275. **Reference:** CVE-2016-2476	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/199
+Priv	2016-06-12	6.8	The Broadcom Wi-Fi driver in Android before 2016-06-01 on Nexus 5, Nexus 6, Nexus 6P, Nexus 7 (2013), Nexus 9, Nexus Player, and Pixel C devices allows attackers to gain privileges for certain system calls via a crafted application, aka internal bug 26425765. **Reference:** CVE-2016-2475	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/200
+Priv	2016-06-12	9.3	The Qualcomm Wi-Fi driver in Android before 2016-06-01 on Nexus 5X devices allows attackers to gain privileges via a crafted application, aka internal bug 27424603. **Reference:** CVE-2016-2474	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/201
+Priv	2016-06-12	9.3	The Qualcomm Wi-Fi driver in Android before 2016-06-01 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka internal bug 27777501. **Reference:** CVE-2016-2473	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/202
+Priv	2016-06-12	9.3	The Qualcomm Wi-Fi driver in Android before 2016-06-01 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka internal bug 27776888. **Reference:** CVE-2016-2472	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/203

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

+Priv	2016-06-12	9.3	The Qualcomm Wi-Fi driver in Android before 2016-06-01 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka internal bug 27773913. **Reference:** CVE-2016-2471	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/204
+Priv	2016-06-12	9.3	The Qualcomm Wi-Fi driver in Android before 2016-06-01 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka internal bug 27662174. **Reference:** CVE-2016-2470	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/205
+Priv	2016-06-12	9.3	The Qualcomm sound driver in Android before 2016-06-01 on Nexus 5, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 27531992. **Reference:** CVE-2016-2469	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/206
+Priv	2016-06-12	9.3	The Qualcomm GPU driver in Android before 2016-06-01 on Nexus 5, 5X, 6, 6P, and 7 devices allows attackers to gain privileges via a crafted application, aka internal bug 27475454. **Reference:** CVE-2016-2468	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/207
+Priv	2016-06-12	9.3	The Qualcomm sound driver in Android before 2016-06-01 on Nexus 5 devices allows attackers to gain privileges via a crafted application, aka internal bug 28029010. **Reference:** CVE-2016-2467	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/208
+Priv	2016-06-12	9.3	The Qualcomm sound driver in Android before 2016-06-01 on Nexus 6 devices allows attackers to gain privileges via a crafted application, aka internal bug 27947307. **Reference:** CVE-2016-2466	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/209
+Priv	2016-06-12	9.3	The Qualcomm video driver in Android before 2016-06-01 on Nexus 5, 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 27407865. **Reference:** CVE-2016-2465	http://source.android.com/security/bulletin/2016-06-01.html	O-GOO-ANDRO-270616/210
DoS Exec Code Mem. Corr.	2016-06-12	9.3	libvpx in libwebm 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 2016-06-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted mkv file, aka internal bug 23167726. **Reference:** CVE-2016-2464	https://android.googlesource.com/platform/external/libvpx/+/cc274e2abe8b2a6698a5c47d8aa4bb45f1f9538d	O-GOO-ANDRO-270616/211
DoS Exec Code Overflow Mem. Corr.	2016-06-12	7.5	Multiple integer overflows in the h264dec component 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 2016-06-01 allow	https://android.googlesource.com/platform/frameworks/av/+/2b6f2	O-GOO-ANDRO-270616/

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

			remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file that triggers a large memory allocation, aka internal bug 27855419. **Reference:** CVE-2016-2463	2dc64d456471a1dc6df09d515771d1427c8	212
Linux					
Linux Kernel: Linux is a kernel for Unix-like operating systems, often called Linux distributions.					
DoS Overflow +Priv Mem. Corr.	2016-06-12	9.3	Integer signedness error in the MSM QDSP6 audio 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 (memory corruption) via a crafted application that makes an ioctl call. **Reference:** CVE-2016-2066	http://source.android.com/security/bulletin/2016-06-01.html	O-LIN-LINUX-270616/213
DoS Overflow +Priv Mem. Corr.	2016-06-12	9.3	Integer signedness error in the MSM V4L2 video 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 (array overflow and memory corruption) via a crafted application that triggers an msm_isp_axi_create_stream call. **Reference:** CVE-2016-2061	https://www.codeaurora.org/array-overflow-msm-v4l2-video-driver-allows-kernel-memory-corruption-cve-2016-2061	O-LIN-LINUX-270616/214
Application					
Citrix					
Xenserver: XenServer is the leading open source virtualization platform, powered by the Xen hypervisor.					
NA	2016-06-13	7.5	Citrix XenServer 7.0 before Hotfix XS70E003, when a deployment has been upgraded from an earlier release, might allow remote attackers on the management network to "compromise" a host by leveraging credentials for an Active Directory account. **Reference:** CVE-2016-5302	http://support.citrix.com/article/CTX213549	A-CIT-XENSE-270616/215
OS					
Huawei					
Rse6500 Firmware;Vp9600 Series Firmware: NA					
Exec Code Overflow	2016-06-13	9.3	Buffer overflow in Huawei VP9660, VP9650, and VP9630 multipoint control unit devices with software before V500R002C00SPC200 and RSE6500 videoconference devices with software before V500R002C00SPC100, when an unspecified service is enabled, allows remote attackers to execute arbitrary code via a crafted packet, aka HWPSIRT-2016-05054. **Reference:** CVE-2016-5234	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160601-01-videoconference-en	O-HUA-RSE65-270616/216

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

Application;OS

Libimobiledevice/Novell

Libimobiledevice;Libusbmuxd/Leap;Opensuse:
Libimobiledevice is a cross-platform protocol library to communicate with iOS devices.openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.

Bypass	2016-06-13	5	The socket_create function in common/socket.c in libimobiledevice and libusbmuxd allows remote attackers to bypass intended access restrictions and communicate with services on iOS devices by connecting to an IPv4 TCP socket. **Reference:** CVE-2016-5104	https://bugzilla.redhat.com/show_bug.cgi?id=1339988	A-LIB-LIBIM-270616/217

Application

Openstack Project

Openstack Identity: Keystone is an OpenStack identity service that manages user databases and OpenStack service catalogs and their API endpoints.

Bypass	2016-06-13	4	The Fernet Token Provider in OpenStack Identity (Keystone) 9.0.x before 9.0.1 (mitaka) allows remote authenticated users to prevent revocation of a chain of tokens and bypass intended access restrictions by rescoping a token. **Reference:** CVE-2016-4911	https://review.openstack.org/#/c/311886/	A-OPE-OPENS-270616/218

OS;Application

Canonical/Libksba Project

Ubuntu Linux/Libskba: Ubuntu is an open source software platform. Libksba allows remote attackers to cause a denial of service (out-of-bounds read and crash) via unspecified vectors.

DoS	2016-06-13	5	Libksba before 1.3.4 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via unspecified vectors, related to the "returned length of the object from _ksba_ber_parse_tl." **Reference:** CVE-2016-4579	http://git.gnupg.org/cgi-bin/gitweb.cgi?p=libksba.git;a=commit;h=a7eed17a0b2a1c09ef986f3b4b323cd31cea2b64	O-CAN-UBUNT-270616/219
DoS	2016-06-13	5	Off-by-one error in the append_utf8_value function in the DN decoder (dn.c) in Libksba before 1.3.4 allows remote attackers to cause a denial of service (out-of-bounds read) via invalid utf-8 encoded data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-4356. **Reference:** CVE-2016-4574	http://git.gnupg.org/cgi-bin/gitweb.cgi?p=libksba.git;a=commit;h=6be61daac047d8e6aa941eb103f8e71a1d4e3c75	O-CAN-UBUNT-270616/220

Application;OS

Atheme/Novell

Atheme/Leap;Opensuse: Atheme is a feature-packed, extremely customisable IRC services daemon that is secure, stable and scalable. LEAP Legal Software provides a completely integrated Legal Case Management & Legal Accounting Solution.openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.

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

DoS Overflow	2016-06-13	5	Buffer overflow in the xmlrpc_char_encode function in modules/transport/xmlrpc/xmlrpclib.c in Atheme before 7.2.7 allows remote attackers to cause a denial of service via vectors related to XMLRPC response encoding. **Reference:** CVE-2016-4478	https://github.com/atheme/atheme/commit/87580d767868360d2fed503980129504da84b63e	A-ATH-ATHEM-270616/221
Fedoraproject;Novell/Quassel-irc					
Fedora/Leap;Opensuse/Quassel: LEAP Legal Software provides a completely integrated Legal Case Management & Legal Accounting Solution.openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.Quassel (sometimes referred to as Quassel IRC) is a cross-platform IRC client introduced in 2008.					
DoS	2016-06-13	5	The onReadyRead function in core/coreauthhandler.cpp in Quassel before 0.12.4 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via invalid handshake data. **Reference:** CVE-2016-4414	http://quassel-irc.org/node/129	O-FED-FEDOR-270616/222
Canonical/Libksba Project					
Ubuntu Linux/Libskba: Ubuntu is an open source software platform. Libksba allows remote attackers to cause a denial of service (out-of-bounds read and crash) via unspecified vectors.					
DoS Overflow	2016-06-13	5	The append_utf8_value function in the DN decoder (dn.c) in Libksba before 1.3.3 allows remote attackers to cause a denial of service (out-of-bounds read) by clearing the high bit of the byte after invalid utf-8 encoded data. **Reference:** CVE-2016-4356	http://git.gnupg.org/cgi-bin/gitweb.cgi?p=libksba.git;a=commit;h=243d12fdec66a4360fbb3e307a046b39b5b4ffc3	O-CAN-UBUNT-270616/223
DoS Overflow	2016-06-13	5	Multiple integer overflows in ber-decoder.c in Libksba before 1.3.3 allow remote attackers to cause a denial of service (crash) via crafted BER data, which leads to a buffer overflow. **Reference:** CVE-2016-4355	http://git.gnupg.org/cgi-bin/gitweb.cgi?p=libksba.git;a=commit;h=aea7b6032865740478ca4b706850a5217f1c3887	O-CAN-UBUNT-270616/224
DoS Overflow	2016-06-13	5	ber-decoder.c in Libksba before 1.3.3 uses an incorrect integer data type, which allows remote attackers to cause a denial of service (crash) via crafted BER data, which leads to a buffer overflow. **Reference:** CVE-2016-4354	http://git.gnupg.org/cgi-bin/gitweb.cgi?p=libksba.git;a=commit;h=aea7b6032865740478ca4b706850a5217f1c3887	O-CAN-UBUNT-270616/225
DoS Overflow	2016-06-13	5	ber-decoder.c in Libksba before 1.3.3 does not properly handle decoder stack overflows, which allows remote attackers to cause a denial of service (abort) via crafted BER data. **Reference:** CVE-2016-4353	http://git.gnupg.org/cgi-bin/gitweb.cgi?p=libksba.git;a=commit;h=07116a314f4dcd4d96990bbd74db95a03a9f650a	O-CAN-UBUNT-270616/226
NA	2016-06-13	0	The Huawei Hilink App application before 3.19.2 for Android does not validate SSL certificates, which allows local users to have unspecified	http://www.huawei.com/en/psirt/security-	O-CAN-UBUNT-

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

		🟩	impact via unknown vectors, aka HWPSIRT-2016-03008. **Reference:** CVE-2016-4005	advisories/huawei-sa-20160419-01-wear-en	270616/227
Canonical;Debian;Redhat/Libndp					
Ubuntu Linux/Debian Linux/Enterprise Linux Desktop;Enterprise Linux Hpc Node;Enterprise Linux Hpc Node Eus;Enterprise Linux Server;Enterprise Linux Server Aus;Enterprise Linux Server Eus;Enterprise Linux Workstation/Libndp: Ubuntu is an open source software platform. Red Hat Enterprise Linux for HPC Compute Nodes works out of the box with an established ecosystem of hardware and software vendors. A Linux server is a high-powered variant of the Linux open source operating system that's designed to handle the more demanding needs of business applications such as network and system administration, database management and Web services. The libndp package provides a wrapper for IPv6 Neighbor Discovery Protocol					
DoS	2016-06-13	6.8	libndp before 1.6, as used in NetworkManager, does not properly validate the origin of Neighbor Discovery Protocol (NDP) messages, which allows remote attackers to conduct man-in-the-middle attacks or cause a denial of service (network connectivity disruption) by advertising a node as a router from a non-local network. **Reference:** CVE-2016-3698	https://github.com/jpirko/libndp/commit/a4892df306e0532487f1634ba6d4c6d4bb381c7f	O-CAN-UBUNT-270616/228
Application					
Huawei					
Hilink App;Wear App: HUAWEI HiLink APP is a new version for both MobileWiFi APP and RuMate APP. The Android Wear app connects your iPhone to your Android Wear watch.					
NA	2016-06-13	6.8	The Huawei Wear App application before 15.0.0.307 for Android does not validate SSL certificates, which allows local users to have unspecified impact via unknown vectors, aka HWPSIRT-2016-03008. **Reference:** CVE-2016-3677	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160419-01-wear-en	A-HUA-HILIN-270616/229
Liferay					
Liferay Portal: Liferay Portal CE is the open source version of Liferay's enterprise web platform for building business solutions					
XSS	2016-06-13	4.3	Cross-site scripting (XSS) vulnerability in users.jsp in the Profile Search functionality in Liferay before 7.0.0 CE RC1 allows remote attackers to inject arbitrary web script or HTML via the FirstName field. **Reference:** CVE-2016-3670	https://issues.liferay.com/browse/LPS-62387	A-LIF-LIFER-270616/230
Mozilla					
Firefox;Network Security Services: Firefox is a free web browser. Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications					
DoS Mem. Corr.	2016-06-13	9.3	Mozilla Network Security Services (NSS) before 3.23, as used in Mozilla Firefox before 47.0, allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact	http://www.mozilla.org/security/announce/2016/mfsa2016-61.html	A-MOZ-FIREF-270616/

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

		🟥	via unknown vectors. **Reference:** CVE-2016-2834		231
XSS	2016-06-13	4.3	Mozilla Firefox before 47.0 ignores Content Security Policy (CSP) directives for cross-domain Java applets, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via a crafted applet. **Reference:** CVE-2016-2833	http://www.mozilla.org/security/announce/2016/mfsa2016-60.html	A-MOZ-FIREF-270616/232
+Info	2016-06-13	4.3	Mozilla Firefox before 47.0 allows remote attackers to discover the list of disabled plugins via a fingerprinting attack involving Cascading Style Sheets (CSS) pseudo-classes. **Reference:** CVE-2016-2832	http://www.mozilla.org/security/announce/2016/mfsa2016-59.html	A-MOZ-FIREF-270616/233
DoS	2016-06-13	5.8	Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 do not ensure that the user approves the fullscreen and pointerlock settings, which allows remote attackers to cause a denial of service (UI outage), or conduct clickjacking or spoofing attacks, via a crafted web site. **Reference:** CVE-2016-2831	http://www.mozilla.org/security/announce/2016/mfsa2016-58.html	A-MOZ-FIREF-270616/234
	2016-06-13	4.3	Mozilla Firefox before 47.0 allows remote attackers to spoof permission notifications via a crafted web site that rapidly triggers permission requests, as demonstrated by the microphone permission or the geolocation permission. **Reference:** CVE-2016-2829	http://www.mozilla.org/security/announce/2016/mfsa2016-57.html	A-MOZ-FIREF-270616/235
Exec Code	2016-06-13	6.8	Use-after-free vulnerability in Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 allows remote attackers to execute arbitrary code via WebGL content that triggers texture access after destruction of the texture's recycle pool. **Reference:** CVE-2016-2828	http://www.mozilla.org/security/announce/2016/mfsa2016-56.html	A-MOZ-FIREF-270616/236
+Priv	2016-06-13	6.9	The maintenance service in Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 on Windows does not prevent MAR extracted-file modification during updater execution, which might allow local users to gain privileges via a Trojan horse file. **Reference:** CVE-2016-2826	http://www.mozilla.org/security/announce/2016/mfsa2016-55.html	A-MOZ-FIREF-270616/237
Bypass	2016-06-13	0	Mozilla Firefox before 47.0 allows remote attackers to bypass the Same Origin Policy and modify the location.host property via an invalid data: URL. **Reference:** CVE-2016-2825	http://www.mozilla.org/security/announce/2016/mfsa2016-54.html	A-MOZ-FIREF-270616/238
DoS Overflow	2016-06-13	6.8	The TSymbolTableLevel class in ANGLE, as used in Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 on Windows, allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact by triggering use of a WebGL shader that writes to an array. **Reference:** CVE-2016-2824	http://www.mozilla.org/security/announce/2016/mfsa2016-53.html	A-MOZ-FIREF-270616/239

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

NA	2016-06-13	0	Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 allow remote attackers to spoof the address bar via a SELECT element with a persistent menu. **Reference:** CVE-2016-2822	http://www.mozilla.org/security/announce/2016/mfsa2016-52.html	A-MOZ-FIREF-270616/240
DoS Exec Code Mem. Corr.	2016-06-13	0	Use-after-free vulnerability in the mozilla::dom::Element class in Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2, when contenteditable mode is enabled, allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by triggering deletion of DOM elements that were created in the editor. **Reference:** CVE-2016-2821	http://www.mozilla.org/security/announce/2016/mfsa2016-51.html	A-MOZ-FIREF-270616/241
Exec Code Overflow	2016-06-13	6.8	Heap-based buffer overflow in Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 allows remote attackers to execute arbitrary code via foreign-context HTML5 fragments, as demonstrated by fragments within an SVG element. **Reference:** CVE-2016-2819	http://www.mozilla.org/security/announce/2016/mfsa2016-50.html	A-MOZ-FIREF-270616/242
DoS Exec Code Overflow Mem. Corr.	2016-06-13	6.8	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors. **Reference:** CVE-2016-2818	http://www.mozilla.org/security/announce/2016/mfsa2016-49.html	A-MOZ-FIREF-270616/243
DoS Exec Code Mem. Corr.	2016-06-13	0	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 47.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors. **Reference:** CVE-2016-2815	http://www.mozilla.org/security/announce/2016/mfsa2016-49.html	A-MOZ-FIREF-270616/244
Apache					
Ranger: Designed specifically for education, Ranger Software provides everything you need to manage your ICT network and equipment					
Exec Code Sql	2016-06-13	6.5	SQL injection vulnerability in the policy admin tool in Apache Ranger before 0.5.3 allows remote authenticated administrators to execute arbitrary SQL commands via the eventTime parameter to service/plugins/policies/eventTime. **Reference:** CVE-2016-2174	https://cwiki.apache.org/confluence/display/RANGER/Vulnerabilities+found+in+Ranger	A-APA-RANGE-270616/245
BMC					
Bladelogic Server Automation Console: BladeLogic Server Automation, one of BMC's digital enterprise automationsolutions, allows you to quickly and securely provision, configure, patch, and maintain physical, virtual, and cloud servers.					
Bypass	2016-06-13	5	The RPC API in RSCD agent in BMC BladeLogic Server Automation (BSA) 8.2.x, 8.3.x, 8.5.x, 8.6.x, and 8.7.x on Linux and UNIX allows remote attackers to bypass authorization and reset arbitrary user passwords by sending an action	https://selfservice.bmc.com/casemgmt/sc_KnowledgeArticle?sfdcid=kA214000000dBpn	A-BMC-BLADE-270616/

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

			packet to xmlrpc after an authorization failure. **Reference:** CVE-2016-1543	CAE&type=Solution	246
Bypass	2016-06-13	5	The RPC API in RSCD agent in BMC BladeLogic Server Automation (BSA) 8.2.x, 8.3.x, 8.5.x, 8.6.x, and 8.7.x on Linux and UNIX allows remote attackers to bypass authorization and enumerate users by sending an action packet to xmlrpc after an authorization failure. **Reference:** CVE-2016-1542	https://selfservice.bmc.com/casemgmt/sc_KnowledgeArticle?sfdcid=kA214000000dBpnCAE&type=Solution	A-BMC-BLADE-270616/247
OS;Application					
Fedoraproject;Novell/Ocaml					
Fedora/Opensuse/Ocaml: OCaml originally known as Objective Caml, is the main implementation of the Caml programming language. Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project. openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.					
Overflow +Info	2016-06-13	6.4	OCamel before 4.03.0 does not properly handle sign extensions, which allows remote attackers to conduct buffer overflow attacks or obtain sensitive information as demonstrated by a long string to the String.copy function. **Reference:** CVE-2015-8869	https://github.com/ocaml/ocaml/commit/659615c7b100a89eafe6253e7a5b9d84d0e8df74#diff-a97df53e3ebc59bb457191b496c90762	O-FED-FEDOR-270616/248
Atheme/Novell					
Atheme/Leap;Opensuse: Atheme is a feature-packed, extremely customisable IRC services daemon that is secure, stable and scalable. LEAP Legal Software provides a completely integrated Legal Case Management & Legal Accounting Solution.openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.					
NA	2016-06-13	5	modules/chanserv/flags.c in Atheme before 7.2.7 allows remote attackers to modify the Anope FLAGS behavior by registering and dropping the (1) LIST, (2) CLEAR, or (3) MODIFY keyword nicks. **Reference:** CVE-2014-9773	https://github.com/atheme/atheme/commit/c597156adc60a45b5f827793cd420945f47bc03b	A-ATH-ATHEM-270616/249
OS					
Huawei					
Honor Ws851 Firmware: Huawei Honor WS851 routers with software 1.1.21.1 and earlier allow remote attackers to modify configuration data via vectors related to a "file injection vulnerability," aka HWPSIRT-2016-05052.					
+Info	2016-06-14	5	Huawei Honor WS851 routers with software 1.1.21.1 and earlier allow remote attackers to obtain sensitive information via unspecified vectors, aka HWPSIRT-2016-05053. **Reference:** CVE-2016-5367	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160607-01-honorrouter-en	O-HUA-HONOR-270616/250
	2016-06-14	5	Huawei Honor WS851 routers with software 1.1.21.1 and earlier allow remote attackers to modify configuration data via vectors related to a "file injection vulnerability," aka HWPSIRT-2016-05052.	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160607-	O-HUA-HONOR-270616/

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

			Reference: CVE-2016-5366	01-honorrouter-en	251
Exec Code Overflow	2016-06-14	10	Stack-based buffer overflow in Huawei Honor WS851 routers with software 1.1.21.1 and earlier allows remote attackers to execute arbitrary commands with root privileges via unspecified vectors, aka HWPSIRT-2016-05051. **Reference:** CVE-2016-5365	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160607-01-honorrouter-en	O-HUA-HONOR-270616/252
Application					
Qemu					
Qemu: QEMU (short for Quick Emulator) is a free and open-source hosted hypervisor that performs hardware virtualization QEMU is a hosted virtual machine monitor					
DoS Exec Code	2016-06-14	4.6	The (1) esp_reg_read and (2) esp_reg_write functions in hw/scsi/esp.c in QEMU allow local guest OS administrators to cause a denial of service (QEMU process crash) or execute arbitrary code on the QEMU host via vectors related to the information transfer buffer. **Reference:** CVE-2016-5338	http://git.qemu.org/?p=qemu.git;a=commit;h=ff589551c8e8e9e95e211b9d8daafb4ed39f1aec	A-QEM-QEMU-270616/253
+Info	2016-06-14	2.1	The megasas_ctrl_get_info function in hw/scsi/megasas.c in QEMU allows local guest OS administrators to obtain sensitive host memory information via vectors related to reading device control information. **Reference:** CVE-2016-5337	http://git.qemu.org/?p=qemu.git;a=commit;h=844864fbae66935951529408831c2f22367a57b6	A-QEM-QEMU-270616/254
DoS Overflow	2016-06-14	2.1	The get_cmd function in hw/scsi/esp.c in QEMU might allow local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) via vectors related to reading from the information transfer buffer in non-DMA mode. **Reference:** CVE-2016-5238	https://bugzilla.redhat.com/show_bug.cgi?id=1341931	A-QEM-QEMU-270616/255

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