Vulnerability Summary for the Week of March 20, 2017

Please Note:

- The vulnerabilities are cattegorized by their level of severity which is either High, Medium or Low.
- The CVE indentity number is the publicly known ID given to that particular vulnerability. Therefore you can search the status of that particular vulnerability using that ID.
- The CVSS (Common Vulnerability Scoring System) score is a standard scoring system used to determine the severity of the vulnerability.

High Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
canonical -- ubuntu_linux	The ReadPSDLayers function in coders/psd.c in ImageMagick 6.8.9.9 allows remote attackers to have unspecified impact via unknown vectors, related to "throwing of exceptions."	2017-03-20	7.5	CVE-2014-9841 SUSE SUSE SUSE MLIST (link is external) UBUNTU (link is external) CONFIRM CONFIRM (link is external)
canonical -- ubuntu_linux	The DecodePSDPixels function in coders/psd.c in ImageMagick 6.8.9.9 allows remote attackers to have unspecified impact via unknown vectors.	2017-03-20	7.5	CVE-2014-9843 SUSE SUSE SUSE MLIST (link is external) UBUNTU (link is external) CONFIRM CONFIRM (link is external)
canonical -- ubuntu_linux	Buffer overflow in the ReadRLEImage function in coders/rle.c in ImageMagick 6.8.9.9 allows remote attackers to have unspecified impact.	2017-03-20	7.5	CVE-2014-9846 SUSE SUSE

				SUSE SUSE SUSE SUSE SUSE SUSE MLIST (link is external) UBUNTU (link is external) CONFIRM CONFIRM (link is external)
canonical -- ubuntu_linux	The jng decoder in ImageMagick 6.8.9.9 allows remote attackers to have an unspecified impact.	2017-03-20	7.5	CVE-2014-9847 SUSE SUSE SUSE SUSE SUSE SUSE MLIST (link is external) UBUNTU (link is external) CONFIRM CONFIRM (link is external)
cerberus -- cerberus_ftp_server	Buffer overflow in Cerberus FTP Server 8.0.10.3 allows remote attackers to cause a denial of service (daemon crash) or possibly have unspecified other impact via a long MLST command.	2017-03-17	7.5	CVE-2017-6880 EXPLOIT-DB (link is external)
chef_manage_project -- chef_manage	The user-account creation feature in Chef Manage 2.1.0 through 2.4.4 allows remote attackers to execute arbitrary code. This is fixed in 2.4.5.	2017-03-17	7.5	CVE-2017-7174 CONFIRM (link is external)
erlang -- erlang/otp	An issue was discovered in Erlang/OTP 18.x. Erlang's generation of compiled regular expressions is vulnerable to a heap overflow. Regular expressions using a malformed extpattern can indirectly specify an offset that is used as an array index. This ordinal permits arbitrary regions within the erts_alloc arena to be both read and written to.	2017-03-18	7.5	CVE-2016-10253 MISC (link is external)
gnu -- binutils	ihex.c in GNU Binutils before 2.26 contains a	2017-03-21	7.5	CVE-2014-9939

	stack buffer overflow when printing bad bytes in Intel Hex objects.			MISC (link is external) CONFIRM CONFIRM
gnu -- screen	GNU screen before 4.5.1 allows local users to modify arbitrary files and consequently gain root privileges by leveraging improper checking of logfile permissions.	2017-03-20	7.2	CVE-2017-5618 CONFIRM CONFIRM CONFIRM MLIST (link is external) BID (link is external) MLIST
ibm -- power_hardware_management_console	IBM Power Hardware Management Console (HMC) 3.3.2 and 4.1 could allow a local user to escalate their privileges to gain root access. IBM Reference #: 1998459.	2017-03-20	7.2	CVE-2017-1134 CONFIRM (link is external) BID (link is external)
ibm -- websphere_mq	IBM WebSphere MQ 8.0.0.6 does not properly terminate channel agents when they are no longer needed, which could allow a user to cause a denial of service through resource exhaustion. IBM Reference #: 1999672.	2017-03-20	7.8	CVE-2017-1145 CONFIRM (link is external) BID (link is external)
imagemagick -- imagemagick	distribute-cache.c in ImageMagick re-uses objects after they have been destroyed, which allows remote attackers to have unspecified impact via unspecified vectors.	2017-03-17	7.5	CVE-2014-9852 SUSE SUSE SUSE MLIST (link is external) CONFIRM CONFIRM (link is external)
imagemagick -- imagemagick	Memory leak in the NewXMLTree function in magick/xml-tree.c in ImageMagick before 6.9.4-7 allows remote attackers to cause a denial of service (memory consumption) via a crafted XML file.	2017-03-23	7.1	CVE-2016-10047 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	Memory leak in the ReadPSDLayers function in coders/psd.c in ImageMagick before 6.9.6-3 allows remote attackers to cause a denial of service (memory consumption) via a crafted	2017-03-23	7.1	CVE-2016-10058 MLIST (link is external) BID (link is external)

	image file.			CONFIRM (link is external) CONFIRM (link is external)
juniper -- junos_space	Insufficient authentication vulnerability in Junos Space before 15.2R2 allows remote network based users with access to Junos Space web interface to perform certain administrative tasks without authentication.	2017-03-20	7.5	CVE-2016-4926 BID (link is external) CONFIRM (link is external)
juniper -- junos_space	Command injection vulnerability in Junos Space before 15.2R2 allows attackers to execute arbitrary code as a root user.	2017-03-20	9.0	CVE-2016-4929 BID (link is external) CONFIRM (link is external)
kinsey -- infor-lawson	Multiple SQL injection vulnerabilities in Kinsey Infor-Lawson (formerly ESBUS) allow remote attackers to execute arbitrary SQL commands via the (1) TABLE parameter to esbus/servlet/GetSQLData or (2) QUERY parameter to KK_LS9ReportingPortal/GetData.	2017-03-20	7.5	CVE-2017-6550 MISC (link is external) FULLDISC BID (link is external) EXPLOIT-DB (link is external)
linux -- linux_kernel	The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel through 4.10.4 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a large command size in an SG_NEXT_CMD_LEN ioctl call, leading to out-of-bounds write access in the sg_write function.	2017-03-20	7.2	CVE-2017-7187 BID (link is external) MISC (link is external) MISC
netiq -- access_governance_suite	A logged-in user in NetIQ Access Governance Suite 6.0 through 6.4 could escalate privileges to administrator.	2017-03-23	9.0	CVE-2016-1597 CONFIRM (link is external)
netiq -- access_manager	iManager Admin Console in NetIQ Access Manager 4.1 before 4.1.2 Hot Fix 1 and 4.2 before 4.2.2 was vulnerable to iFrame manipulation attacks, which could allow remote users to gain access to authentication credentials.	2017-03-23	7.5	CVE-2016-5757 CONFIRM (link is external)
oneplus -- oxygenos	An issue was discovered in OxygenOS before 4.1.0 on OnePlus 3 and 3T devices. The attacker can change the bootmode of the device by issuing the 'fastboot oem boot_mode	2017-03-19	7.2	CVE-2017-5623 BID (link is external) MISC (link is external)

	{rf/wlan/ftm/normal} command' in contradiction to the threat model of Android where the bootloader MUST NOT allow any security-sensitive operation to be run unless the bootloader is unlocked.			
openinfosecfoundation -- suricata	The MemcmpLowercase function in Suricata before 2.0.6 improperly excludes the first byte from comparisons, which might allow remote attackers to bypass intrusion-prevention functionality via a crafted HTTP request.	2017-03-20	7.5	CVE-2015-8954 CONFIRM CONFIRM CONFIRM
pluck-cms -- pluck	Pluck CMS 4.7.2 allows remote attackers to execute arbitrary code via the blog form feature.	2017-03-17	7.5	CVE-2014-8708 MISC (link is external) MISC (link is external)
qdpm -- qdpm	Unrestricted file upload vulnerability in the (1) myAccount, (2) projects, (3) tasks, (4) tickets, (5) discussions, (6) reports, and (7) scheduler pages in qdPM 8.3 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in uploads/attachments/ or uploads/users/.	2017-03-17	7.5	CVE-2015-3884 MISC (link is external) MISC (link is external)
wondercms -- wondercms	Directory traversal vulnerability in index.php in Wonder CMS 2014 allows remote attackers to include and execute arbitrary local files via a crafted theme.	2017-03-17	7.5	CVE-2014-8704 MISC (link is external)
wondercms -- wondercms	PHP remote file inclusion vulnerability in editInplace.php in Wonder CMS 2014 allows remote attackers to execute arbitrary PHP code via a URL in the hook parameter.	2017-03-17	7.5	CVE-2014-8705 MISC (link is external) MISC (link is external)
xrdp -- xrdp	xrdp 0.9.1 calls the PAM function auth_start_session() in an incorrect location, leading to PAM session modules not being properly initialized, with a potential consequence of incorrect configurations or elevation of privileges, aka a pam_limits.so bypass.	2017-03-17	7.5	CVE-2017-6967 MISC (link is external) MISC (link is external) MISC (link is external)

Medium Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
apache -- tomcat	The code in Apache Tomcat 9.0.0.M1 to 9.0.0.M11, 8.5.0 to 8.5.6, 8.0.0.RC1 to 8.0.38, 7.0.0 to 7.0.72, and 6.0.0 to 6.0.47 that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response. By manipulating the HTTP response the attacker could poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other then their own.	2017-03-20	6.8	CVE-2016-6816 BID (link is external) CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
apng2gif_project -- apng2gif	An issue was discovered in apng2gif 1.7. There is an integer overflow resulting in a heap-based buffer over-read, related to the load_apng function and the imagesize variable.	2017-03-17	5.0	CVE-2017-6960 MISC
apng2gif_project -- apng2gif	An issue was discovered in apng2gif 1.7. There is improper sanitization of user input causing huge memory allocations, resulting in a crash. This is related to the read_chunk function using the pChunk->size value (within the PNG file) to determine the amount of memory to allocate.	2017-03-17	4.3	CVE-2017-6961 MISC
apng2gif_project -- apng2gif	An issue was discovered in apng2gif 1.7. There is an integer overflow resulting in a heap-based buffer overflow. This is related to the read_chunk function making an unchecked addition of 12.	2017-03-17	5.0	CVE-2017-6962 MISC
artifex -- ghostscript	The mem_get_bits_rectangle function in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (NULL pointer	2017-03-21	4.3	CVE-2017-7207 CONFIRM (link is external) BID (link is external)

	dereference) via a crafted PostScript document.			CONFIRM (link is external)
audiofile -- audiofile	The decodeSample function in IMA.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-20	4.3	CVE-2017-6829 MLIST (link is external) MISC MISC (link is external) MISC (link is external)
audiofile -- audiofile	Heap-based buffer overflow in the alaw2linear_buf function in G711.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-20	4.3	CVE-2017-6830 MLIST (link is external) MISC MISC (link is external) MISC (link is external)
audiofile -- audiofile	Heap-based buffer overflow in the decodeBlockWAVE function in IMA.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-20	4.3	CVE-2017-6831 MLIST (link is external) MISC MISC (link is external) MISC (link is external)
audiofile -- audiofile	Heap-based buffer overflow in the decodeBlock in MSADPCM.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-20	4.3	CVE-2017-6832 MLIST (link is external) MISC MISC (link is external) MISC (link is external)
audiofile -- audiofile	The runPull function in libaudiofile/modules/BlockCodec.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (divide-by-zero error and crash) via a crafted file.	2017-03-20	4.3	CVE-2017-6833 MLIST (link is external) MISC MISC (link is external) MISC (link is external)
audiofile -- audiofile	Heap-based buffer overflow in the ulaw2linear_buf function in G711.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-20	4.3	CVE-2017-6834 MLIST (link is external) MISC MISC (link is external) MISC (link is

				external)
audiofile -- audiofile	The reset1 function in libaudiofile/modules/BlockCodec.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (divide-by-zero error and crash) via a crafted file.	2017-03-20	4.3	CVE-2017-6835 MLIST (link is external) MISC MISC (link is external) MISC (link is external)
audiofile -- audiofile	Heap-based buffer overflow in the Expand3To4Module::run function in libaudiofile/modules/SimpleModule.h in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-20	4.3	CVE-2017-6836 MLIST (link is external) MISC MISC (link is external) MISC (link is external)
audiofile -- audiofile	WAVE.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via vectors related to a large number of coefficients.	2017-03-20	4.3	CVE-2017-6837 MLIST (link is external) MISC MISC (link is external) MISC (link is external)
audiofile -- audiofile	Integer overflow in sfcommands/sfconvert.c in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-20	4.3	CVE-2017-6838 MLIST (link is external) MISC MISC (link is external) MISC (link is external)
audiofile -- audiofile	Integer overflow in modules/MSADPCM.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-20	4.3	CVE-2017-6839 MLIST (link is external) MISC MISC (link is external) MISC (link is external)
buddypress -- buddypress_plugin	An issue was discovered in includes/component.php in the BuddyPress Docs plugin before 1.9.3 for WordPress. It is possible for authenticated users to edit documents of other users without proper permissions.	2017-03-17	4.0	CVE-2017-6954 CONFIRM (link is external) CONFIRM
ca --	The get_sessions servlet in CA Unified Infrastructure	2017-03-20	5.0	CVE-2016-9165 BID (link is

unified_infrastructure_management	Management (formerly CA Nimsoft Monitor) before 8.5 and CA Unified Infrastructure Management Snap (formerly CA Nimsoft Monitor Snap) allows remote attackers to obtain active session ids and consequently bypass authentication or gain privileges via unspecified vectors.			external) MISC (link is external) CONFIRM (link is external)
canonical -- ubuntu_linux	Memory leak in the ReadPSDLayers function in coders/psd.c in ImageMagick 6.8.9.9 allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors.	2017-03-20	5.0	CVE-2014-9842 SUSE SUSE SUSE SUSE MLIST (link is external) CONFIRM CONFIRM (link is external)
canonical -- ubuntu_linux	The ReadRLEImage function in coders/rle.c in ImageMagick 6.8.9.9 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted image file.	2017-03-20	4.3	CVE-2014-9844 SUSE SUSE SUSE SUSE SUSE SUSE MLIST (link is external) UBUNTU (link is external) CONFIRM CONFIRM (link is external)
canonical -- ubuntu_linux	The ReadDIBImage function in coders/dib.c in ImageMagick allows remote attackers to cause a denial of service (crash) via a corrupted dib file.	2017-03-20	4.3	CVE-2014-9845 SUSE SUSE SUSE SUSE SUSE SUSE SUSE SUSE MLIST (link is external) UBUNTU (link is external) CONFIRM CONFIRM (link is external)
canonical -- ubuntu_linux	Memory leak in ImageMagick allows remote attackers to cause a denial of service (memory	2017-03-20	5.0	CVE-2014-9848 SUSE

	consumption).			SUSE SUSE SUSE SUSE MLIST (link is external) UBUNTU (link is external) CONFIRM (link is external)
canonical -- ubuntu_linux	The png coder in ImageMagick allows remote attackers to cause a denial of service (crash).	2017-03-20	5.0	CVE-2014-9849 SUSE SUSE SUSE SUSE MLIST (link is external) UBUNTU (link is external) CONFIRM (link is external)
canonical -- ubuntu_linux	Logic error in ImageMagick 6.8.9.9 allows remote attackers to cause a denial of service (resource consumption).	2017-03-20	5.0	CVE-2014-9850 SUSE SUSE SUSE MLIST (link is external) UBUNTU (link is external) CONFIRM CONFIRM (link is external)
canonical -- ubuntu_linux	ImageMagick 6.8.9.9 allows remote attackers to cause a denial of service (application crash).	2017-03-20	5.0	CVE-2014-9851 SUSE SUSE SUSE SUSE MLIST (link is external) UBUNTU (link is external) CONFIRM CONFIRM (link is external)
cisco -- adaptive_security_appliance_software	A vulnerability in the Border Gateway Protocol (BGP) Bidirectional Forwarding Detection (BFD) implementation of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to bypass the	2017-03-17	5.0	CVE-2017-3867 BID (link is external) CONFIRM (link is external)

	access control list (ACL) for specific TCP and UDP traffic. More Information: CSCvc68229. Known Affected Releases: 9.6(2). Known Fixed Releases: 99.1(20.1) 99.1(10.2) 98.1(12.7) 98.1(1.49) 97.1(6.58) 97.1(0.134) 96.2(0.109) 9.7(1.1) 9.6(2.99) 9.6(2.8).			
cisco -- nx-os	An Access-Control Filtering Mechanisms Bypass vulnerability in certain access-control filtering mechanisms on Cisco Nexus 7000 Series Switches could allow an unauthenticated, remote attacker to bypass defined traffic configured within an access control list (ACL) on the affected system. More Information: CSCtz59354. Known Affected Releases: 5.2(4) 6.1(3)S5 6.1(3)S6 6.2(1.121)S0 7.2(1)D1(1) 7.3(0)ZN(0.161) 7.3(1)N1(0.1). Known Fixed Releases: 7.3(0)D1(1) 6.2(2) 6.1(5) 8.3(0)KMT(0.24) 8.3(0)CV(0.337) 7.3(1)N1(1) 7.3(0)ZN(0.210) 7.3(0)ZN(0.177) 7.3(0)ZD(0.194) 7.3(0)TSH(0.99) 7.3(0)SC(0.14) 7.3(0)RSP(0.7) 7.3(0)N1(1) 7.3(0)N1(0.193) 7.3(0)IZN(0.13) 7.3(0)IB(0.102) 7.3(0)GLF(0.44) 7.3(0)D1(0.178) 7.1(0)D1(0.14) 7.0(3)ITI2(1.6) 7.0(3)ISH1(2.13) 7.0(3)IFD6(0.78) 7.0(3)IFD6(0) 7.0(3)IDE6(0.12) 7.0(3)IDE6(0) 7.0(3)I2(1) 7.0(3)I2(0.315) 7.0(1)ZD(0.3) 7.0(0)ZD(0.84) 6.2(1.149)S0 6.2(0.285) 6.1(5.32)S0 6.1(4.97)S0 6.1(2.30)S0.	2017-03-17	5.0	CVE-2017-3875 BID (link is external) CONFIRM (link is external)
cisco -- nx-os	A Denial of Service vulnerability in the Telnet remote login functionality of Cisco NX-OS Software running on Cisco Nexus 9000 Series Switches could allow an unauthenticated, remote attacker to cause a Telnet process used for login to terminate unexpectedly and the login attempt to fail. There is no impact to user traffic flowing through the device. Affected Products: This vulnerability affects Cisco Nexus 9000 Series Switches that are running Cisco NX-OS Software and are configured to allow remote Telnet connections to the device. More Information: CSCux46778. Known Affected Releases: 7.0(3)I3(0.170). Known Fixed Releases: 7.0(3)I3(1) 7.0(3)I3(0.257) 7.0(3)I3(0.255) 7.0(3)I2(2e)	2017-03-17	5.0	CVE-2017-3878 BID (link is external) CONFIRM (link is external)

	7.0(3)F1(1.22) 7.0(3)F1(1).			
cisco -- nx-os	A Denial of Service vulnerability in the remote login functionality for Cisco NX-OS Software running on Cisco Nexus 9000 Series Switches could allow an unauthenticated, remote attacker to cause a process used for login to terminate unexpectedly and the login attempt to fail. There is no impact to user traffic flowing through the device. The attacker could use either a Telnet or an SSH client for the remote login attempt. Affected Products: This vulnerability affects Cisco Nexus 9000 Series Switches that are running Cisco NX-OS Software and are configured to allow remote Telnet connections to the device. More Information: CSCuy25824. Known Affected Releases: 7.0(3)I3(1) 8.3(0)CV(0.342) 8.3(0)CV(0.345). Known Fixed Releases: 8.3(0)CV(0.362) 8.0(1) 7.0(3)IED5(0.19) 7.0(3)IED5(0) 7.0(3)I4(1) 7.0(3)I4(0.8) 7.0(3)I2(2e) 7.0(3)F1(1.22) 7.0(3)F1(1) 7.0(3)F1(0.230).	2017-03-17	5.0	CVE-2017-3879 BID (link is external) CONFIRM (link is external)
cisco -- prime_infrastructure	An API Credentials Management vulnerability in the APIs for Cisco Prime Infrastructure could allow an authenticated, remote attacker to access an API that should be restricted to a privileged user. The attacker needs to have valid credentials. More Information: CSCuy36192. Known Affected Releases: 3.1(1) 3.1(1).	2017-03-17	5.5	CVE-2017-3869 BID (link is external) CONFIRM (link is external)
cisco -- prime_optical	A RADIUS Secret Disclosure vulnerability in the web network management interface of Cisco Prime Optical for Service Providers could allow an authenticated, remote attacker to disclose sensitive information in the configuration generated for a device. The attacker must have valid credentials for the device. More Information: CSCvc65257. Known Affected Releases: 10.6(0.1).	2017-03-17	4.0	CVE-2017-3871 BID (link is external) CONFIRM (link is external)
cisco -- prime_service_catalog	A vulnerability in the web framework code of Cisco Prime Service Catalog could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against the user of the web interface of the affected system. More	2017-03-17	4.3	CVE-2017-3866 BID (link is external) CONFIRM (link is external)

	Information: CSCvc79842 CSCvc79846 CSCvc79855 CSCvc79873 CSCvc79882 CSCvc79891. Known Affected Releases: 11.1.2.			
cisco -- telepresence_server_software	An API Privilege vulnerability in Cisco TelePresence Server Software could allow an unauthenticated, remote attacker to emulate Cisco TelePresence Server endpoints. Affected Products: This vulnerability affects Cisco TelePresence Server MSE 8710 Processors that are running a software release prior to Cisco TelePresence Software Release 4.3 and are running in locally managed mode. The vulnerable API was deprecated in Cisco TelePresence Software Release 4.3. More Information: CSCvc37616.	2017-03-17	5.0	CVE-2017-3815 BID (link is external) CONFIRM (link is external)
cisco -- unified_communications_manager	A cross-site scripting (XSS) filter bypass vulnerability in the web-based management interface of Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to conduct XSS attacks against a user of an affected device. More Information: CSCvc21620. Known Affected Releases: 10.5(2.14076.1). Known Fixed Releases: 12.0(0.98000.641) 12.0(0.98000.500) 12.0(0.98000.219).	2017-03-17	4.3	CVE-2017-3872 BID (link is external) CONFIRM (link is external)
cisco -- unified_communications_manager	A vulnerability in the web framework of Cisco Unified Communications Manager (CallManager) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web interface of the affected software. More Information: CSCvb70021. Known Affected Releases: 11.5(1.11007.2).	2017-03-17	4.3	CVE-2017-3877 BID (link is external) CONFIRM (link is external)
cisco -- unified_computing_system_director	A vulnerability in the web-based management interface of Cisco UCS Director could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. More Information: CSCvc44344. Known Affected Releases: 6.0(0.0).	2017-03-17	4.3	CVE-2017-3868 BID (link is external) CONFIRM (link is external)
cisco --	A vulnerability in the URL filtering feature of Cisco	2017-03-17	5.0	CVE-2017-3870 BID (link is

web_security_appliance	AsyncOS Software for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to bypass a configured URL filter rule. Affected Products: This vulnerability affects all releases prior to the first fixed release of Cisco AsyncOS Software for Cisco Web Security Appliance (WSA), both virtual and hardware appliances, that are configured with URL filters for email scanning. More Information: CSCvc69700. Known Affected Releases: 8.5.3-069 9.1.1-074 9.1.2-010.			external) CONFIRM (link is external)
cisco -- webex_meetings_server	An XML External Entity vulnerability in Cisco WebEx Meetings Server could allow an authenticated, remote attacker to have read access to part of the information stored in the affected system. More Information: CSCvc39165. Known Affected Releases: 2.6. Known Fixed Releases: 2.7.1.2054.	2017-03-17	4.0	CVE-2017-3811 BID (link is external) CONFIRM (link is external)
cisco -- webex_meetings_server	An Authentication Bypass vulnerability in Cisco WebEx Meetings Server could allow an unauthenticated, remote attacker to access limited meeting information on the Cisco WebEx Meetings Server. More Information: CSCvd50728. Known Affected Releases: 2.6 2.7 2.8 CWMS-2.5MR1 Orion1.1.2.patch T29_orion_merge.	2017-03-17	6.4	CVE-2017-3880 BID (link is external) CONFIRM (link is external)
cloudflare-scrape_project -- cloudflare-scrape	An issue was discovered in cloudflare-scrape 1.6.6 through 1.7.1. A malicious website owner could craft a page that executes arbitrary Python code against any cfscrape user who scrapes that website. This is fixed in 1.8.0.	2017-03-23	6.8	CVE-2017-7235 CONFIRM (link is external) CONFIRM (link is external)
d-link -- dir-600m_firmware	CSRF exists on D-Link DIR-600M Rev. Cx devices before v3.05ENB01_beta_20170306. This can be used to bypass authentication and insert XSS sequences or possibly have unspecified other impact.	2017-03-22	6.8	CVE-2017-5874 CONFIRM (link is external) BID (link is external)
debian -- debian_linux	The IsPixelGray function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3-8 allows remote attackers to cause a denial of service (out-of-bounds heap read) via a crafted image file.	2017-03-23	4.3	CVE-2016-9556 SUSE DEBIAN MLIST (link is external) MLIST (link is external)

				MLIST (link is external) BID (link is external) MISC CONFIRM (link is external) CONFIRM (link is external)
deluge -- deluge	CSRF was discovered in the web UI in Deluge before 1.3.14. The exploitation methodology involves (1) hosting a crafted plugin that executes an arbitrary program from its __init__.py file and (2) causing the victim to download, install, and enable this plugin.	2017-03-18	6.8	CVE-2017-7178 CONFIRM MISC MISC MISC BID (link is external) CONFIRM
fedoraproject -- fedora	Integer overflow in the read_fragment_table_4 function in unsquash-4.c in Squashfs and sasquatch allows remote attackers to cause a denial of service (application crash) via a crafted input, which triggers a stack-based buffer overflow.	2017-03-17	4.3	CVE-2015-4645 FEDORA FEDORA BID (link is external) CONFIRM (link is external) MISC (link is external) GENTOO
ffmpeg -- ffmpeg	Libavcodec in FFmpeg before 0.11 allows remote attackers to cause a denial of service (memory corruption and application crash) or execute arbitrary code.	2017-03-20	6.8	CVE-2012-5361 BID (link is external) XF (link is external) MS (link is external) CONFIRM
gamepanelx -- gamepanelx-v3	A Cross-Site Scripting (XSS) was discovered in GamePanelX-V3 3.0.12. The vulnerability exists due to insufficient filtration of user-supplied data (a) passed to the "GamePanelX-V3-master/ajax/ajax.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-21	4.3	CVE-2017-7205 BID (link is external) CONFIRM (link is external)
get-simple -- getsimple_cms	GetSimple CMS 3.3.4 allows remote attackers to obtain sensitive information via a direct request to (1) data/users/<username>.xml, (2) backups/users/<username>.xml.bak, (3)	2017-03-17	5.0	CVE-2014-8722 MISC (link is external) MISC (link is external)

	data/other/authorization.xml, or (4) data/other/appid.xml.			
get-simple -- getsimple_cms	GetSimple CMS 3.3.4 allows remote attackers to obtain sensitive information via a direct request to (1) plugins/anonymous_data.php or (2) plugins/InnovationPlugin.php, which reveals the installation path in an error message.	2017-03-17	5.0	CVE-2014-8723 MISC (link is external) MISC (link is external)
git_project -- git	contrib/completion/git-prompt.sh in Git before 1.9.3 does not sanitize branch names in the PS1 variable, allowing a malicious repository to cause code execution.	2017-03-19	6.8	CVE-2014-9938 CONFIRM (link is external) MISC (link is external)
gnu -- binutils	readelf in GNU Binutils 2.28 writes to illegal addresses while processing corrupt input files containing symbol-difference relocations, leading to a heap-based buffer overflow.	2017-03-17	4.3	CVE-2017-6965 CONFIRM
gnu -- binutils	readelf in GNU Binutils 2.28 has a use-after-free (specifically read-after-free) error while processing multiple, relocated sections in an MSP430 binary. This is caused by mishandling of an invalid symbol index, and mishandling of state across invocations.	2017-03-17	4.3	CVE-2017-6966 CONFIRM
gnu -- binutils	readelf in GNU Binutils 2.28 is vulnerable to a heap-based buffer over-read while processing corrupt RL78 binaries. The vulnerability can trigger program crashes. It may lead to an information leak as well.	2017-03-17	6.4	CVE-2017-6969 CONFIRM
gnu -- binutils	The dump_section_as_bytes function in readelf in GNU Binutils 2.28 accesses a NULL pointer while reading section contents in a corrupt binary, leading to a program crash.	2017-03-21	4.3	CVE-2017-7209 BID (link is external) CONFIRM
gnu -- binutils	objdump in GNU Binutils 2.28 is vulnerable to multiple heap-based buffer over-reads (of size 1 and size 8) while handling corrupt STABS enum type strings in a crafted object file, leading to program crash.	2017-03-21	4.3	CVE-2017-7210 BID (link is external) CONFIRM
gnu -- binutils	GNU assembler in GNU Binutils 2.28 is vulnerable to a global buffer overflow (of size 1) while attempting to unget an EOF character from the input stream, potentially leading to a program crash.	2017-03-22	5.0	CVE-2017-7223 CONFIRM

gnu -- binutils	The find_nearest_line function in objdump in GNU Binutils 2.28 is vulnerable to an invalid write (of size 1) while disassembling a corrupt binary that contains an empty function name, leading to a program crash.	2017-03-22	4.3	CVE-2017-7224 CONFIRM
gnu -- binutils	The find_nearest_line function in addr2line in GNU Binutils 2.28 does not handle the case where the main file name and the directory name are both empty, triggering a NULL pointer dereference and an invalid write, and leading to a program crash.	2017-03-22	5.0	CVE-2017-7225 CONFIRM
gnu -- binutils	The pe_ILF_object_p function in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to a heap-based buffer over-read of size 4049 because it uses the strlen function instead of strnlen, leading to program crashes in several utilities such as addr2line, size, and strings. It could lead to information disclosure as well.	2017-03-22	6.4	CVE-2017-7226 CONFIRM
gnu -- binutils	GNU linker (ld) in GNU Binutils 2.28 is vulnerable to a heap-based buffer overflow while processing a bogus input script, leading to a program crash. This relates to lack of '\0' termination of a name field in ldlex.l.	2017-03-22	5.0	CVE-2017-7227 CONFIRM
gnu -- glibc	Integer overflow in the _IO_wstr_overflow function in libio/wstrops.c in the GNU C Library (aka glibc or libc6) before 2.22 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to computing a size in bytes, which triggers a heap-based buffer overflow.	2017-03-20	6.8	CVE-2015-8983 MLIST (link is external) BID (link is external) CONFIRM CONFIRM MLIST
gnu -- glibc	The fnmatch function in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent attackers to cause a denial of service (application crash) via a malformed pattern, which triggers an out-of-bounds read.	2017-03-20	4.3	CVE-2015-8984 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM MLIST

gnu -- glibc	The pop_fail_stack function in the GNU C Library (aka glibc or libc6) allows context-dependent attackers to cause a denial of service (assertion failure and application crash) via vectors related to extended regular expression processing.	2017-03-20	4.3	CVE-2015-8985 MLIST (link is external) BID (link is external) CONFIRM
google -- android	The Qualcomm SPCom driver in Android before 7.0 allows local users to execute arbitrary code within the context of the kernel via a crafted application, aka Android internal bug 34386529 and Qualcomm internal bug CR#1094140.	2017-03-20	6.9	CVE-2016-5857 SECTRACK (link is external) MISC (link is external)
huawei -- document_security_management	The permission control module in Huawei Document Security Management (aka DSM) before V100R002C05SPC670 allows remote authenticated users to obtain sensitive information from encrypted documents by leveraging incorrect control of permissions on the PrintScreen button.	2017-03-20	4.0	CVE-2016-2406 CONFIRM (link is external)
ibm -- algo_one	IBM Algorithmics One-Algo Risk Application 4.9.1, 5.0, and 5.1.0 could allow a user to gain access to another user's reports using a specially crafted HTTP request. IBM Reference #: 1999754.	2017-03-20	4.0	CVE-2017-1155 CONFIRM (link is external) BID (link is external)
ibm -- rational_rhapsody_design_manager	IBM Rhapsody DM 4.0, 5.0 and 6.0 contains an undisclosed vulnerability that may allow an authenticated user to upload infected malicious files to the server. IBM Reference #: 1999960.	2017-03-20	4.0	CVE-2016-8973 CONFIRM (link is external) BID (link is external)
ibm -- websphere_application_server	IBM WebSphere Application Server 8.0, 8.5, 8.5.5, and 9.0 using OpenID Connect (OIDC) configured with a Trust Association Interceptor (TAI) could allow a user to gain elevated privileges on the system. IBM Reference #: 1999293.	2017-03-20	6.8	CVE-2017-1151 CONFIRM (link is external) BID (link is external)
imagemagick -- imagemagick	Heap overflow in ImageMagick 6.8.9-9 via a crafted pcx file.	2017-03-22	6.8	CVE-2014-9832 MLIST (link is external) MLIST (link is external)
imagemagick -- imagemagick	Heap overflow in ImageMagick 6.8.9-9 via a crafted psd file.	2017-03-22	6.8	CVE-2014-9833 MLIST (link is external) MLIST (link is external)
imagemagick --	Heap overflow in ImageMagick 6.8.9-9 via a crafted	2017-03-22	6.8	CVE-2014-9834

imagemagick	pict file.			MLIST (link is external) MLIST (link is external)
imagemagick -- imagemagick	Heap overflow in ImageMagick 6.8.9-9 via a crafted wpf file.	2017-03-22	6.8	CVE-2014-9835 MLIST (link is external) MLIST (link is external)
imagemagick -- imagemagick	ImageMagick 6.8.9-9 allows remote attackers to cause a denial of service via a crafted xpm file.	2017-03-22	4.3	CVE-2014-9836 MLIST (link is external) MLIST (link is external)
imagemagick -- imagemagick	magick/cache.c in ImageMagick 6.8.9-9 allows remote attackers to cause a denial of service (crash).	2017-03-22	4.3	CVE-2014-9838 MLIST (link is external)
imagemagick -- imagemagick	magick/colormap-private.h in ImageMagick 6.8.9-9 allows remote attackers to cause a denial of service (out-of-bounds access).	2017-03-22	5.0	CVE-2014-9839 MLIST (link is external) MLIST (link is external)
imagemagick -- imagemagick	ImageMagick 6.8.9-9 allows remote attackers to cause a denial of service (out-of-bounds access) via a crafted palm file.	2017-03-22	4.3	CVE-2014-9840 MLIST (link is external) MLIST (link is external)
imagemagick -- imagemagick	Memory leak in coders/rle.c in ImageMagick allows remote attackers to cause a denial of service (memory consumption) via a crafted rle file.	2017-03-17	4.3	CVE-2014-9853 SUSE SUSE SUSE SUSE SUSE SUSE SUSE SUSE MLIST (link is external) UBUNTU (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	coders/tiff.c in ImageMagick allows remote attackers to cause a denial of service (application crash) via vectors related to the "identification of image."	2017-03-17	5.0	CVE-2014-9854 CONFIRM SUSE SUSE SUSE SUSE MLIST (link is

				external) UBUNTU (link is external) CONFIRM CONFIRM (link is external)
imagemagick -- imagemagick	Off-by-one error in ImageMagick before 6.6.0-4 allows remote attackers to cause a denial of service (application crash) via a crafted 8BIM profile.	2017-03-23	4.3	CVE-2014-9915 MLIST (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	Heap-based buffer overflow in the DrawImage function in magick/draw.c in ImageMagick before 6.9.5-5 allows remote attackers to cause a denial of service (application crash) via a crafted image file.	2017-03-23	4.3	CVE-2016-10046 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	Buffer overflow in the ReadRLEImage function in coders/rle.c in ImageMagick before 6.9.4-4 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted RLE file.	2017-03-23	6.8	CVE-2016-10049 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) MISC
imagemagick -- imagemagick	Buffer overflow in the WriteProfile function in coders/jpeg.c in ImageMagick before 6.9.5-6 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.	2017-03-23	6.8	CVE-2016-10052 SUSE SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	The WriteTIFFImage function in coders/tiff.c in ImageMagick before 6.9.5-8 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted file.	2017-03-23	4.3	CVE-2016-10053 MLIST (link is external) BID (link is external)

				CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	Buffer overflow in the WriteMAPImage function in coders/map.c in ImageMagick before 6.9.5-8 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.	2017-03-23	6.8	CVE-2016-10054 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	Buffer overflow in the WritePDBImage function in coders/pdb.c in ImageMagick before 6.9.5-8 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.	2017-03-23	6.8	CVE-2016-10055 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	Buffer overflow in the sixel_decode function in coders/sixel.c in ImageMagick before 6.9.5-8 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.	2017-03-23	6.8	CVE-2016-10056 MLIST (link is external) BID (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	Buffer overflow in the WriteGROUP4Image function in coders/tiff.c in ImageMagick before 6.9.5-8 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.	2017-03-23	6.8	CVE-2016-10057 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	Buffer overflow in coders/tiff.c in ImageMagick before 6.9.4-1 allows remote attackers to cause a denial of service (application crash) or have	2017-03-23	6.8	CVE-2016-10059 SUSE MLIST (link is

	unspecified other impact via a crafted TIFF file.			external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
imdbphp_project -- imdbphp	A Cross-Site Scripting (XSS) was discovered in imdbphp 5.1.1. The vulnerability exists due to insufficient filtration of user-supplied data (name) passed to the "imdbphp-master/demo/search.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-21	4.3	CVE-2017-7204 BID (link is external) CONFIRM (link is external)
jasper_project -- jasper	The bmp_getdata function in libjasper/bmp/bmp_dec.c in JasPer before 1.900.9 allows remote attackers to cause a denial of service (NULL pointer dereference) by calling the imginfo command with a crafted BMP image.	2017-03-23	4.3	CVE-2016-8885 MLIST (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) MISC CONFIRM (link is external) FEDORA FEDORA
juniper -- junos_space	Insufficient validation of SSH keys in Junos Space before 15.2R2 allows man-in-the-middle (MITM) type of attacks while a Space device is communicating with managed devices.	2017-03-20	6.8	CVE-2016-4927 BID (link is external) CONFIRM (link is external)
juniper -- junos_space	Cross site request forgery vulnerability in Junos Space before 15.2R2 allows remote attackers to perform certain administrative actions on Junos Space.	2017-03-20	6.8	CVE-2016-4928 BID (link is external) CONFIRM (link is external)
juniper -- junos_space	Cross-site scripting (XSS) vulnerability in Junos Space before 15.2R2 allows remote attackers to steal sensitive information or perform certain administrative actions.	2017-03-20	4.3	CVE-2016-4930 BID (link is external) CONFIRM (link is external)
juniper -- junos_space	XML entity injection in Junos Space before 15.2R2 allows attackers to cause a denial of service.	2017-03-20	4.0	CVE-2016-4931 BID (link is external) CONFIRM (link

				is external)
libav -- libav	The ff_h2645_extract_rbsp function in libavcodec in libav 9.21 allows remote attackers to cause a denial of service (heap-based buffer over-read) or obtain sensitive information from process memory via a crafted h264 video file.	2017-03-21	5.8	CVE-2017-7206 BID (link is external) CONFIRM
libav -- libav	The decode_residual function in libavcodec in libav 9.21 allows remote attackers to cause a denial of service (buffer over-read) or obtain sensitive information from process memory via a crafted h264 video file.	2017-03-21	5.8	CVE-2017-7208 BID (link is external) CONFIRM
libtiff -- libtiff	LibTIFF allows remote attackers to cause a denial of service (memory consumption and crash) via a crafted tiff file.	2017-03-17	4.3	CVE-2015-7313 MLIST BID (link is external) CONFIRM (link is external) GENTOO
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in MantisBT before 2.1.1 allows remote attackers to inject arbitrary HTML or JavaScript (if MantisBT's CSP settings permit it) by modifying 'window_title' in the application configuration. This requires privileged access to MantisBT configuration management pages (i.e., administrator access rights) or altering the system configuration file (config_inc.php).	2017-03-22	4.3	CVE-2017-7222 CONFIRM (link is external) CONFIRM
mantisbt -- mantisbt_source_integration_plugin	An XSS vulnerability in the MantisBT Source Integration Plugin (before 2.0.2) search result page allows an attacker to inject arbitrary HTML or JavaScript (if MantisBT's CSP settings permit it) by crafting any valid parameter.	2017-03-17	4.3	CVE-2017-6958 CONFIRM (link is external)
meteocontrol -- weblog	A Cross-Site Request Forgery issue was discovered in Meteocontrol WEB'log Basic 100 all versions, Light all versions, Pro all versions, and Pro Unlimited all versions. There is no CSRF Token generated per page or per function.	2017-03-21	6.8	CVE-2016-4504 MISC
misp -- misp	Cross site scripting in some view elements in the index filter tool in app/webroot/js/misp2.4.68.js and the organisation landing page in	2017-03-21	4.3	CVE-2017-7215 MISC (link is external)

	app/View/Organisations/ajax/landingpage.ctp of MISP before 2.4.69 allows remote attackers to inject arbitrary web script or HTML.			BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
mobatek -- mobaxterm	Directory traversal vulnerability in the TFTP server in MobaXterm Personal Edition 9.4 allows remote attackers to read arbitrary files via a .. (dot dot) in a GET command.	2017-03-20	5.0	CVE-2017-6805 MISC MISC (link is external) FULLDISC BID (link is external) EXPLOIT-DB (link is external)
netiq -- access_manager	The certificate upload feature in iManager in NetIQ Access Manager 4.1 before 4.1.2 Hot Fix 1 and 4.2 before 4.2.2 could be used to upload JSP pages that would be executed as the iManager user, allowing code execution by logged-in remote users.	2017-03-23	6.5	CVE-2016-5750 CONFIRM (link is external)
netiq -- access_manager	An unfiltered finalizer target URL in the SAML processing feature in Identity Server in NetIQ Access Manager 4.1 before 4.1.2 HF1 and 4.2 before 4.2.2 could be used to trigger XSS and leak authentication credentials.	2017-03-23	4.3	CVE-2016-5751 CONFIRM (link is external)
netiq -- access_manager	The SAML2 implementation in Identity Server in NetIQ Access Manager 4.1 before 4.1.2 HF1 and 4.2 before 4.2.2 was handling unsigned SAML requests incorrectly, leaking results to a potentially malicious "Assertion Consumer Service URL" instead of the original requester.	2017-03-23	5.0	CVE-2016-5752 CONFIRM (link is external)
netiq -- access_manager	Presence of a .htaccess file could leak information in NetIQ Access Manager 4.1 before 4.1.2 Hot Fix 1 and 4.2 before SP2.	2017-03-23	5.0	CVE-2016-5754 CONFIRM (link is external)
netiq -- access_manager	NetIQ Access Manager 4.1 before 4.1.2 Hot Fix 1 and 4.2 before 4.2.2 was vulnerable to clickjacking attacks due to a missing SAMEORIGIN filter in the "high encryption" setting.	2017-03-23	4.3	CVE-2016-5755 CONFIRM (link is external)

netiq -- access_manager	Multiple components of the web tools in NetIQ Access Manager 4.1 before 4.1.2 Hot Fix 1 and 4.2 before 4.2.2 were vulnerable to Reflected Cross Site Scripting attacks which could be used to hijack user sessions: nps/servlet/frameservice, nps/servlet/webacc, roma/admin/cntl, roma/jsp/admin/appliance/devicedetail_edit.jsp, roma/jsp/admin/managementip/mgmt_ip_details_frameset.jsp, roma/jsp/admin/managementip/mgmt_ip_details_middleframe.jsp, roma/jsp/volsc/monitoring/appliance.jsp, and roma/jsp/volsc/monitoring/graph.jsp.	2017-03-23	4.3	CVE-2016-5756 CONFIRM (link is external)
netiq -- access_manager	A cross site request forgery protection mechanism in NetIQ Access Manager 4.1 before 4.1.2 Hot Fix 1 and 4.2 before 4.2.2 could be circumvented by repeated uploads causing a high load.	2017-03-23	6.8	CVE-2016-5758 BID (link is external) CONFIRM (link is external)
novell -- groupwise	A reflected XSS vulnerability exists in the web console of the Document Viewer Agent in Novell GroupWise before 2014 R2 Support Pack 1 Hot Patch 2 that may enable a remote attacker to execute JavaScript in the context of a valid user's browser session by getting the user to click on a specially crafted link. This could lead to session compromise or other browser-based attacks.	2017-03-23	4.3	CVE-2016-9169 CONFIRM (link is external)
novell -- leap	saned in sane-backends 1.0.25 allows remote attackers to obtain sensitive memory information via a crafted SANE_NET_CONTROL_OPTION packet.	2017-03-20	5.0	CVE-2017-6318 MLIST MLIST SUSE BID (link is external) CONFIRM MLIST
opendaylight -- l2switch	hosttracker in OpenDaylight l2switch allows remote attackers to change the host location information by spoofing the MAC address, aka "topology spoofing."	2017-03-20	5.0	CVE-2015-1610 MISC BID (link is external) CONFIRM
openinfosecfoundation -- suricata	Suricata before 3.2.1 has an IPv4 defragmentation evasion issue caused by lack of a check for the IP protocol during fragment matching.	2017-03-18	5.0	CVE-2017-7177 BID (link is external) CONFIRM (link

				is external) CONFIRM
openstack -- nova	An issue was discovered in exception_wrapper.py in OpenStack Nova 13.x through 13.1.3, 14.x through 14.0.4, and 15.x through 15.0.1. Legacy notification exception contexts appearing in ERROR level logs may include sensitive information such as account passwords and authorization tokens.	2017-03-21	5.0	CVE-2017-7214 BID (link is external) CONFIRM (link is external)
opensuse_project -- leap	Directory traversal vulnerability in magick/module.c in ImageMagick 6.9.4-7 allows remote attackers to load arbitrary modules via unspecified vectors.	2017-03-23	5.0	CVE-2016-10048 SUSE SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
opensuse_project -- leap	Heap-based buffer overflow in the ReadRLEImage function in coders/rle.c in ImageMagick 6.9.4-8 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted RLE file.	2017-03-23	6.8	CVE-2016-10050 SUSE SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
opensuse_project -- leap	Use-after-free vulnerability in the ReadPWPImage function in coders/pwp.c in ImageMagick 6.9.5-5 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.	2017-03-23	6.8	CVE-2016-10051 SUSE SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM
palo_alto_networks --	Palo Alto Networks Terminal Services (aka TS) Agent 6.0, 7.0, and 8.0 before 8.0.1 uses weak permissions	2017-03-20	5.0	CVE-2017-6356 CONFIRM (link is external)

terminal_services_agent	for unspecified resources, which allows attackers to obtain sensitive session information via unknown vectors.			BID (link is external)
pcre -- pcre	libpcre1 in PCRE 8.40 and libpcre2 in PCRE2 10.23 allow remote attackers to cause a denial of service (segmentation violation for read access, and application crash) by triggering an invalid Unicode property lookup.	2017-03-19	5.0	CVE-2017-7186 BID (link is external) MISC CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
pluck-cms -- pluck	Pluck CMS 4.7.2 allows remote attackers to obtain sensitive information by (1) changing "PHPSESSIS" to an array; (2) adding non-aplhanumeric chars to "PHPSESSID"; (3) changing the image parameter to array; or (4) changing the image parameter to a string, which reveals the installation path in an error message.	2017-03-17	5.0	CVE-2014-8706 MISC (link is external) MISC (link is external)
pluck-cms -- pluck	Cross-site scripting (XSS) vulnerability in TinyMCE in Pluck CMS 4.7.2 allows remote authenticated users to inject arbitrary web script or HTML via the "edit HTML source" option.	2017-03-17	4.0	CVE-2014-8707 MISC (link is external) MISC (link is external)
qdpm -- qdpm	Information disclosure issue in qdPM 8.3 allows remote attackers to obtain sensitive information via a direct request to (1) core/config/databases.yml, (2) core/log/qdPM_prod.log, or (3) core/apps/qdPM/config/settings.yml.	2017-03-17	5.0	CVE-2015-3881 MISC (link is external) MISC (link is external)
qdpm -- qdpm	qdPM 8.3 allows remote attackers to obtain sensitive information via invalid ID value to index.php/users/info/id/[ID], which reveals the installation path in an error message.	2017-03-17	5.0	CVE-2015-3882 MISC (link is external) MISC (link is external)
qdpm -- qdpm	Multiple cross-site scripting (XSS) vulnerabilities in qdPM 8.3 allow remote attackers to inject arbitrary web script or HTML via the (1) search[keywords] parameter to index.php/users page; the (2) "Name of application" on index.php/configuration; (3) a new project name on index.php/projects; (4) the task name on index.php/tasks; (5) ticket name on index.php/tickets; (6) discussion name on	2017-03-17	4.3	CVE-2015-3883 MISC (link is external) MISC (link is external)

	index.php/discussions; (7) report name on index.php/projectReports; or (8) event name on index.php/scheduler/personal.			
qemu -- qemu	Buffer overflow in NetRxPkt::ehdr_buf in hw/net/net_rx_pkt.c in QEMU (aka Quick Emulator), when the VLANSTRIP feature is enabled on the vmxnet3 device, allows remote attackers to cause a denial of service (out-of-bounds access and QEMU process crash) via vectors related to VLAN stripping.	2017-03-20	5.0	CVE-2017-6058 CONFIRM MLIST (link is external) BID (link is external) SECTRACK (link is external) CONFIRM (link is external) MLIST
sitecore -- experience_platform	Cross-Site Scripting (XSS) in "/sitecore/client/Applications/List Manager/Taskpages/Contact list" in Sitecore Experience Platform 8.1 rev. 160519 (8.1 Update-3) allows remote attacks via the Name or Description parameter. This is fixed in 8.2 Update-2.	2017-03-19	4.3	CVE-2016-8855 MISC (link is external) EXPLOIT-DB (link is external)
slims -- slims7_cendana	Multiple Cross-Site Scripting (XSS) were discovered in SLiMS 7 Cendana before 2017-03-16. The vulnerabilities exist due to insufficient filtration of user-supplied data (id) passed to the 'slims7_cendana-master/template/default/detail_template.php' and 'slims7_cendana-master/template/default-rtl/detail_template.php' URLs. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-21	4.3	CVE-2017-7202 BID (link is external) CONFIRM (link is external)
solarwinds -- ftp_voyager	Multiple cross-site request forgery (CSRF) vulnerabilities in the web interface in the Scheduler in SolarWinds (formerly Serv-U) FTP Voyager 16.2.0 allow remote attackers to hijack the authentication of users for requests that (1) change the admin password, (2) terminate the scheduler, or (3) possibly execute arbitrary commands via crafted requests to Admin/XML/Result.xml.	2017-03-20	6.8	CVE-2017-6803 MISC MISC (link is external) BID (link is external) EXPLOIT-DB (link is external)
teleogistic -- invite_anyone_plugin	An issue was discovered in by-email/by-email.php in the Invite Anyone plugin before 1.3.15 for WordPress. A user is able to change the subject and	2017-03-17	5.0	CVE-2017-6955 BID (link is external) CONFIRM (link

	the body of the invitation mail that should be immutable, which facilitates a social engineering attack.			is external) CONFIRM
typo3 -- typo3	TYPO3 7.6.15 sends an http request to an index.php?loginProvider URI in cases with an https Referer, which allows remote attackers to obtain sensitive cleartext information by sniffing the network and reading the userident and username fields.	2017-03-17	5.0	CVE-2017-6370 MISC (link is external)
usbpcap_project -- usbpcap	The IofCallDriver function in USBPcap 1.1.0.0 allows local users to gain privileges via a crafted 0x00090028 IOCTL call, which triggers a NULL pointer dereference.	2017-03-20	4.6	CVE-2017-6178 MISC (link is external) BID (link is external) EXPLOIT-DB (link is external)
virglrenderer_project -- virglrenderer	Memory leak in the virgl_resource_attach_backing function in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (memory consumption) via a large number of VIRTIO_GPU_CMD_RESOURCE_ATTACH_BACKING commands.	2017-03-20	4.9	CVE-2016-10214 MLIST (link is external) BID (link is external) CONFIRM MLIST
wondercms -- wondercms	Wonder CMS 2014 allows remote attackers to obtain sensitive information by viewing /files/password, which reveals the unsalted MD5 hashed password.	2017-03-17	5.0	CVE-2014-8701 MISC (link is external) MISC (link is external)
wondercms -- wondercms	Wonder CMS 2014 allows remote attackers to obtain sensitive information by logging into the application with an array for the password, which reveals the installation path in an error message.	2017-03-17	5.0	CVE-2014-8702 MISC (link is external) MISC (link is external)
wondercms -- wondercms	Cross-site scripting (XSS) vulnerability in Wonder CMS 2014 allows remote attackers to inject arbitrary web script or HTML.	2017-03-17	4.3	CVE-2014-8703 MISC (link is external) MISC (link is external)
zoneminder -- zoneminder	A Cross-Site Scripting (XSS) was discovered in ZoneMinder 1.30.2. The vulnerability exists due to insufficient filtration of user-supplied data (postLoginQuery) passed to the "ZoneMinder-master/web/skins/classic/views/js/postlogin.js.php"	2017-03-21	4.3	CVE-2017-7203 BID (link is external) CONFIRM (link is external)

	URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.			

Low Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
cisco -- unified_communications_manager	A vulnerability in the web framework of Cisco Unified Communications Manager (CallManager) could allow an authenticated, remote attacker to perform a cross-site scripting (XSS) attack. More Information: CSCvb70033. Known Affected Releases: 11.5(1.11007.2). Known Fixed Releases: 12.0(0.98000.507) 11.0(1.23900.5) 11.0(1.23900.3) 10.5(2.15900.2).	2017-03-17	3.5	CVE-2017-3874 BID (link is external) CONFIRM (link is external)
ibm -- content_navigator	IBM Content Navigator 2.0.3 and 3.0.0 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1999736.	2017-03-20	3.5	CVE-2017-1146 CONFIRM (link is external) BID (link is external)
ibm -- rational_collaborative_lifecycle_management	An undisclosed vulnerability in the CLM applications in IBM Jazz Team Server may allow unauthorized access to user credentials. IBM Reference #: 1999965.	2017-03-20	2.1	CVE-2016-2981 CONFIRM (link is external) MISC (link is external)
ibm -- rational_rhapsody_design_manager	IBM Rhapsody DM 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1999960.	2017-03-20	3.5	CVE-2016-9694 CONFIRM (link is external) BID (link is external)

ibm -- rational_rhapsody_design_manager	IBM Rhapsody DM 4.0, 5.0, and 6.0 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM Reference #: 1999960.	2017-03-20	3.5	CVE-2016-9696 CONFIRM (link is external) BID (link is external)
ibm -- rational_rhapsody_design_manager	An unspecified vulnerability in IBM Rhapsody DM 4.0, 5.0, and 6.0 could allow an attacker to perform a JSON Hijacking Attack. A JSON Hijacking Attack may expose to an attacker information passed between the server and the browser. IBM Reference #: 1999960.	2017-03-20	2.1	CVE-2016-9697 CONFIRM (link is external) BID (link is external)
netiq -- access_manager	External Entity Processing (XXE) vulnerability in the "risk score" application of NetIQ Access Manager 4.1 before 4.1.2 Hot Fix 1 and 4.2 before 4.2.2 could be used to disclose the content of local files to logged-in users.	2017-03-23	2.1	CVE-2016-5748 CONFIRM (link is external)
netiq -- access_manager	NetIQ Access Manager 4.1 before 4.1.2 HF 1 and 4.2 before 4.2.2 was parsing incoming SAML requests with external entity resolution enabled, which could lead to local file disclosure via an XML External Entity (XXE) attack.	2017-03-23	2.1	CVE-2016-5749 CONFIRM (link is external)
opensuse_project -- leap	The AliasHandler component in PostfixAdmin before 3.0.2 allows remote authenticated domain admins to delete protected aliases via the delete parameter to delete.php, involving a missing permission check.	2017-03-20	3.5	CVE-2017-5930 SUSE MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) MLIST (link is external)
qemu -- qemu	The sdhci_sdma_transfer_multi_blocks function in hw/sd/sdhci.c in QEMU (aka Quick Emulator) allows local OS guest privileged users to cause a denial of service (infinite loop and QEMU process crash) via vectors involving the transfer mode register during multi block transfer.	2017-03-20	2.1	CVE-2017-5987 CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link

				is external) MLIST
virglrenderer_project -- virglrenderer	The vrend_draw_vbo function in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (out-of-bounds array access and QEMU process crash) via vectors involving vertext_buffer_index.	2017-03-20	2.1	CVE-2017-5956 MLIST (link is external) BID (link is external) CONFIRM MLIST
cisco -- unified_communications_manager	A vulnerability in the web framework of Cisco Unified Communications Manager (CallManager) could allow an authenticated, remote attacker to perform a cross-site scripting (XSS) attack. More Information: CSCvb70033. Known Affected Releases: 11.5(1.11007.2). Known Fixed Releases: 12.0(0.98000.507) 11.0(1.23900.5) 11.0(1.23900.3) 10.5(2.15900.2).	2017-03-17	3.5	CVE-2017-3874 BID (link is external) CONFIRM (link is external)
ibm -- content_navigator	IBM Content Navigator 2.0.3 and 3.0.0 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1999736.	2017-03-20	3.5	CVE-2017-1146 CONFIRM (link is external) BID (link is external)
ibm -- rational_collaborative_lifecycle_management	An undisclosed vulnerability in the CLM applications in IBM Jazz Team Server may allow unauthorized access to user credentials. IBM Reference #: 1999965.	2017-03-20	2.1	CVE-2016-2981 CONFIRM (link is external) MISC (link is external)
ibm -- rational_rhapsody_design_manager	IBM Rhapsody DM 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1999960.	2017-03-20	3.5	CVE-2016-9694 CONFIRM (link is external) BID (link is external)
ibm -- rational_rhapsody_design_manager	IBM Rhapsody DM 4.0, 5.0, and 6.0 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM Reference #: 1999960.	2017-03-20	3.5	CVE-2016-9696 CONFIRM (link is external) BID (link is external)
ibm --	An unspecified vulnerability in IBM Rhapsody DM	2017-03-20	2.1	CVE-2016-9697

rational_rhapsody_design_manager	4.0, 5.0, and 6.0 could allow an attacker to perform a JSON Hijacking Attack. A JSON Hijacking Attack may expose to an attacker information passed between the server and the browser. IBM Reference #: 1999960.			CONFIRM (link is external) BID (link is external)
netiq -- access_manager	External Entity Processing (XXE) vulnerability in the "risk score" application of NetIQ Access Manager 4.1 before 4.1.2 Hot Fix 1 and 4.2 before 4.2.2 could be used to disclose the content of local files to logged-in users.	2017-03-23	2.1	CVE-2016-5748 CONFIRM (link is external)
netiq -- access_manager	NetIQ Access Manager 4.1 before 4.1.2 HF 1 and 4.2 before 4.2.2 was parsing incoming SAML requests with external entity resolution enabled, which could lead to local file disclosure via an XML External Entity (XXE) attack.	2017-03-23	2.1	CVE-2016-5749 CONFIRM (link is external)
opensuse_project -- leap	The AliasHandler component in PostfixAdmin before 3.0.2 allows remote authenticated domain admins to delete protected aliases via the delete parameter to delete.php, involving a missing permission check.	2017-03-20	3.5	CVE-2017-5930 SUSE MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) MLIST (link is external)
qemu -- qemu	The sdhci_sdma_transfer_multi_blocks function in hw/sd/sdhci.c in QEMU (aka Quick Emulator) allows local OS guest privileged users to cause a denial of service (infinite loop and QEMU process crash) via vectors involving the transfer mode register during multi block transfer.	2017-03-20	2.1	CVE-2017-5987 CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external) MLIST
virglrenderer_project -- virglrenderer	The vrend_draw_vbo function in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (out-of-bounds array access and QEMU process crash) via vectors involving vertext_buffer_index.	2017-03-20	2.1	CVE-2017-5956 MLIST (link is external) BID (link is external) CONFIRM MLIST

- Sources: http://nvd.nist.gov (For more information visit the National Vulnerabilities Database (NVD) which contains a database of every vulnerability that has ever been published).

Uganda Communications Commission – UGCERT
Email: info@ug-cert.ug Tel + 256 414 302 100/150 **Toll Free:** 0800 133 911
Website www.ug-cert.ug Face book / Twitter: UGCERT