Vulnerability Summary for the Week of March 27, 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**
allwinnertech -- linux-3.4-sunxi	The sunxi-debug driver in Allwinner 3.4 legacy kernel for H3, A83T and H8 devices allows local users to gain root privileges by sending "rootmydevice" to /proc/sunxi_debug/sunxi_debug.	2017-03-27	7.2	CVE-2016-10225 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) MISC MISC (link is external)
apache -- camel	Apache Camel's Jackson and JacksonXML unmarshalling operation are vulnerable to Remote Code Execution attacks.	2017-03-28	7.5	CVE-2016-8749 CONFIRM BID (link is external)
apache -- poi	Apache POI in versions prior to release 3.15 allows remote attackers to cause a denial of service (CPU consumption) via a specially crafted OOXML file, aka an XML Entity Expansion (XEE) attack.	2017-03-24	7.1	CVE-2017-5644 CONFIRM BID (link is external)
artifex -- mujs	Heap-based buffer overflow in the	2017-03-24	7.5	CVE-2016-10133

	js_stackoverflow function in jsrun.c in Artifex Software, Inc. MuJS allows attackers to have unspecified impact by leveraging an error when dropping extra arguments to lightweight functions.			CONFIRM (link is external) MLIST (link is external) MLIST (link is external) CONFIRM (link is external) FEDORA
eviewgps -- ev-07s_gps_tracker_firmware	Due to a lack of authentication, an unauthenticated user who knows the Eview EV-07S GPS Tracker's phone number can revert the device to a factory default configuration with an SMS command, "RESET!"	2017-03-27	7.8	CVE-2017-5237 BID (link is external) MISC (link is external)
gnu -- gnutls	Double free vulnerability in the gnutls_x509_ext_import_proxy function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via crafted policy language information in an X.509 certificate with a Proxy Certificate Information extension.	2017-03-24	7.5	CVE-2017-5334 SUSE MLIST (link is external) MLIST (link is external) BID (link is external) SECTRACK (link is external) CONFIRM (link is external) CONFIRM GENTOO
gnu -- gnutls	Stack-based buffer overflow in the cdk_pk_get_keyid function in lib/opencdk/pubkey.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via a crafted OpenPGP certificate.	2017-03-24	7.5	CVE-2017-5336 SUSE MLIST (link is external) MLIST (link is external) BID (link is external) SECTRACK (link is external) MISC CONFIRM (link is external) CONFIRM GENTOO
gnu -- gnutls	Multiple heap-based buffer overflows in the read_attribute function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to have unspecified impact via a crafted OpenPGP	2017-03-24	7.5	CVE-2017-5337 SUSE MLIST (link is external) MLIST (link is external)

	certificate.			BID (link is external) SECTRACK (link is external) MISC MISC CONFIRM (link is external) CONFIRM GENTOO
hesiod_project -- hesiod	The read_config_file function in lib/hesiod.c in Hesiod 3.2.1 falls back to the ".athena.mit.edu" default domain when opening the configuration file fails, which allows remote attackers to gain root privileges by poisoning the DNS cache.	2017-03-28	10.0	CVE-2016-10152 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
huawei -- ar3200_firmware	Huawei AR3200 routers with software before V200R007C00SPC600 allow remote attackers to cause a denial of service or execute arbitrary code via a crafted packet.	2017-03-24	10.0	CVE-2016-6206 CONFIRM (link is external) BID (link is external)
huawei -- mate_s_firmware	The ION driver in Huawei P8 smartphones with software GRA-TL00 before GRA-TL00C01B230, GRA-CL00 before GRA-CL00C92B230, GRA-CL10 before GRA-CL10C92B230, GRA-UL00 before GRA-UL00C00B230, and GRA-UL10 before GRA-UL10C00B230 and Mate S smartphones with software CRR-TL00 before CRR-TL00C01B160SP01, CRR-UL00 before CRR-UL00C00B160, and CRR-CL00 before CRR-CL00C92B161 allows remote attackers to cause a denial of service (crash) via a crafted application.	2017-03-24	7.1	CVE-2015-8678 CONFIRM (link is external)
imagemagick -- imagemagick	coders/ipl.c in ImageMagick allows remote attackers to have unspecific impact by leveraging a missing malloc check.	2017-03-24	7.5	CVE-2016-10144 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM (link is external)

imagemagick -- imagemagick	Off-by-one error in coders/wpg.c in ImageMagick allows remote attackers to have unspecified impact via vectors related to a string copy.	2017-03-24	7.5	CVE-2016-10145 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM (link is external)
imagemagick -- imagemagick	Multiple memory leaks in the caption and label handling code in ImageMagick allow remote attackers to cause a denial of service (memory consumption) via unspecified vectors.	2017-03-24	7.8	CVE-2016-10146 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM (link is external)
imagemagick -- imagemagick	Memory leak in coders/mpc.c in ImageMagick before 6.9.7-4 and 7.x before 7.0.4-4 allows remote attackers to cause a denial of service (memory consumption) via vectors involving a pixel cache.	2017-03-24	7.8	CVE-2017-5507 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	coders/psd.c in ImageMagick allows remote attackers to have unspecified impact by leveraging an improper cast, which triggers a heap-based buffer overflow.	2017-03-24	7.5	CVE-2017-5511 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)

intelliants -- subrion_cms	Subrion CMS 4.0.5.10 has SQL injection in admin/database/ via the query parameter.	2017-03-26	7.5	CVE-2017-6013 BID (link is external) MISC (link is external)
irssi -- irssi	The netjoin processing in Irssi 1.x before 1.0.2 allows attackers to cause a denial of service (use-after-free) and possibly execute arbitrary code via unspecified vectors.	2017-03-27	7.5	CVE-2017-7191 BID (link is external) CONFIRM (link is external) CONFIRM
libgit2_project -- libgit2	Buffer overflow in the git_pkt_parse_line function in transports/smart_pkt.c in the Git Smart Protocol support in libgit2 before 0.24.6 and 0.25.x before 0.25.1 allows remote attackers to have unspecified impact via a crafted non-flush packet.	2017-03-24	7.5	CVE-2016-10128 SUSE SUSE SUSE MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	The vmw_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.6 does not validate addition of certain levels data, which allows local users to trigger an integer overflow and out-of-bounds write, and cause a denial of service (system hang or crash) or possibly gain privileges, via a crafted ioctl call for a /dev/dri/renderD* device.	2017-03-28	7.2	CVE-2017-7294 BID (link is external) MISC (link is external) MISC
linux -- linux_kernel	The packet_set_ring function in net/packet/af_packet.c in the Linux kernel through 4.10.6 does not properly validate certain block-size data, which allows local users to cause a denial of service (overflow) or possibly have unspecified other impact via crafted system calls.	2017-03-29	7.2	CVE-2017-7308 BID (link is external) CONFIRM
microsoft -- iis	Buffer overflow in the ScStoragePathFromUrl	2017-03-26	10.0	CVE-2017-7269

	function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2 allows remote attackers to execute arbitrary code via a long header beginning with "If: <http://" in a PROPFIND request, as exploited in the wild in July or August 2016.			BID (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external)
modx -- modx_revolution	setup/controllers/welcome.php in MODX Revolution 2.5.4-pl and earlier allows remote attackers to execute arbitrary PHP code via the config_key parameter to the setup/index.php?action=welcome URI.	2017-03-30	7.5	CVE-2017-7321 BID (link is external) MISC (link is external)
modx -- modx_revolution	setup/templates/findcore.php in MODX Revolution 2.5.4-pl and earlier allows remote attackers to execute arbitrary PHP code via the core_path parameter.	2017-03-30	7.5	CVE-2017-7324 BID (link is external) MISC (link is external)
moodle -- moodle	In Moodle 2.x and 3.x, SQL injection can occur via user preferences.	2017-03-26	7.5	CVE-2017-2641 BID (link is external) CONFIRM
openbsd -- openbsd	httpd in OpenBSD allows remote attackers to cause a denial of service (memory consumption) via a series of requests for a large file using an HTTP Range header.	2017-03-27	7.8	CVE-2017-5850 MLIST (link is external) MISC (link is external) FULLDISC MLIST (link is external) BID (link is external) SECTRACK (link is external) CONFIRM CONFIRM CONFIRM (link is external) MISC (link is external) EXPLOIT-DB (link is external)
putty -- putty	The ssh_agent_channel_data function in PuTTY before 0.68 allows remote attackers to have unspecified impact via a large length value in an	2017-03-27	7.5	CVE-2017-6542 SUSE CONFIRM BID (link is

	agent protocol message and leveraging the ability to connect to the Unix-domain socket representing the forwarded agent connection, which trigger a buffer overflow.			external) CONFIRM GENTOO
qemu -- qemu	Local privilege escalation vulnerability in the Gentoo QEMU package before 2.5.0-r1.	2017-03-24	10.0	CVE-2015-8556 MISC (link is external) GENTOO EXPLOIT-DB (link is external)
qemu -- qemu	Integer overflow in hw/virtio/virtio-crypto.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (QEMU process crash) or possibly execute arbitrary code on the host via a crafted virtio-crypto request, which triggers a heap-based buffer overflow.	2017-03-27	7.2	CVE-2017-5931 CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external) MLIST
revive-adserver -- revive_adserver	Revive Adserver before 3.2.3 suffers from session fixation, by allowing arbitrary session identifiers to be forced and, at the same time, by not invalidating the existing session upon a successful authentication. Under some circumstances, that could have been an opportunity for an attacker to steal an authenticated session.	2017-03-27	7.5	CVE-2016-9125 MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external)
revive-adserver -- revive_adserver	Revive Adserver before 3.2.5 and 4.0.0 suffers from Reflected File Download. `www/delivery/asyncspc.php` was vulnerable to the fairly new Reflected File Download (RFD) web attack vector that enables attackers to gain complete control over a victim's machine by virtually downloading a file from a trusted domain.	2017-03-27	9.3	CVE-2016-9470 MISC (link is external) MISC (link is external)
solarwinds -- log_and_event_manager	SolarWinds LEM (aka SIEM) before 6.3.1 has an incorrect sudo configuration, which allows local users to obtain root access by editing /usr/local/contego/scripts/hostname.sh.	2017-03-24	7.2	CVE-2017-5198 MISC (link is external) BID (link is external)

Medium Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
amd -- ryzen	The AMD Ryzen processor with AGESA microcode through 2017-01-27 allows local users to cause a denial of service (system hang) via an application that makes a long series of FMA3 instructions, as demonstrated by the Flops test suite.	2017-03-24	4.9	CVE-2017-7262 MISC MISC BID (link is external) MISC (link is external) MISC (link is external)
artifex -- mupdf	Use-after-free vulnerability in the fz_subsample_pixmap function in fitz/pixmap.c in Artifex Software, Inc. MuPDF 1.10a allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted document.	2017-03-26	6.8	CVE-2017-7264 MISC (link is external) BID (link is external) MISC
brave -- browser	Brave Browser iOS before 1.2.18 and Brave Browser Android 1.9.56 and earlier suffer from Full Address Bar Spoofing, allowing attackers to trick a victim by displaying a malicious page for legitimate domain names.	2017-03-27	4.3	CVE-2016-9473 BID (link is external) MISC (link is external) MISC (link is external) MISC (link is external)
broadcom -- bcm4339_soc_firmware	Stack-based buffer overflow in the firmware in Broadcom Wi-Fi HardMAC SoC chips, when the firmware supports CCKM Fast and Secure Roaming and the feature is enabled in RAM, allows remote attackers to execute arbitrary code via a crafted reassociation response frame with a Cisco IE (156).	2017-03-27	6.8	CVE-2017-6957 MISC (link is external) BID (link is external) MISC
call-cc -- chicken	The string-translate* procedure in the data-structures unit in CHICKEN before 4.10.0 allows remote attackers to cause a denial of service (crash).	2017-03-29	5.0	CVE-2015-4556 MLIST MLIST MLIST CONFIRM (link

				is external)
canonical -- ubuntu_core	An issue was discovered in AppArmor before 2.12. Incorrect handling of unknown AppArmor profiles in AppArmor init scripts, upstart jobs, and/or systemd unit files allows an attacker to possibly have increased attack surfaces of processes that were intended to be confined by AppArmor. This is due to the common logic to handle 'restart' operations removing AppArmor profiles that aren't found in the typical filesystem locations, such as /etc/apparmor.d/. Userspace projects that manage their own AppArmor profiles in atypical directories, such as what's done by LXD and Docker, are affected by this flaw in the AppArmor init script logic.	2017-03-24	4.3	CVE-2017-6507 CONFIRM (link is external) CONFIRM (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
clusterlabs -- pacemaker	Pacemaker before 1.1.15, when using pacemaker remote, might allow remote attackers to cause a denial of service (node disconnection) via an unauthenticated connection.	2017-03-24	5.0	CVE-2016-7797 CONFIRM SUSE SUSE SUSE REDHAT (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
debian -- debian_linux	XML External Entity (XXE) vulnerability in PySAML2 4.4.0 and earlier allows remote attackers to read arbitrary files via a crafted SAML XML request or response.	2017-03-24	5.0	CVE-2016-10149 DEBIAN MLIST (link is external) CONFIRM CONFIRM (link is external) MISC (link is external) CONFIRM (link is external)
dotcms -- dotcms	dotCMS 3.7.0 has XSS reachable from ext/languages_manager/edit_language in portal/layout via the bottom two form fields.	2017-03-26	4.3	CVE-2017-6003 BID (link is external) MISC (link is external)

eclipse -- tinydtls	Eclipse tinydtls 0.8.2 for Eclipse IoT allows remote attackers to cause a denial of service (DTLS peer crash) by sending a "Change cipher spec" packet without pre-handshake.	2017-03-24	5.0	CVE-2017-7243 BID (link is external) MISC (link is external) MISC (link is external)
eonweb_project -- eonweb	EyesOfNetwork ("EON") 5.0 and earlier allows remote authenticated users to execute arbitrary code via shell metacharacters in the selected_events[] parameter in the (1) acknowledge, (2) delete, or (3) ownDisown function in module/monitoring_ged/ged_functions.php or the (4) module parameter to module/index.php.	2017-03-24	6.5	CVE-2017-6087 MLIST (link is external) BID (link is external) CONFIRM (link is external)
eviewgps -- ev-07s_gps_tracker_firmware	Due to a lack of bounds checking, several input configuration fields for the Eview EV-07S GPS Tracker will overflow data stored in one variable to another, overwriting the data of another field.	2017-03-27	5.0	CVE-2017-5238 BID (link is external) MISC (link is external)
eviewgps -- ev-07s_gps_tracker_firmware	Due to a lack of standard encryption when transmitting sensitive information over the internet to a centralized monitoring service, the Eview EV-07S GPS Tracker discloses personally identifying information, such as GPS data and IMEI numbers, to any man-in-the-middle (MitM) listener.	2017-03-27	5.0	CVE-2017-5239 BID (link is external) MISC (link is external)
exfat_prokect -- exfat	Heap-based buffer overflow in the verify_vbr_checksum function in exfatfsck in exfat-utils before 1.2.1 allows remote attackers to cause a denial of service (infinite loop) or possibly execute arbitrary code via a crafted filesystem.	2017-03-27	6.8	CVE-2015-8026 MLIST (link is external) BID (link is external) MISC CONFIRM (link is external) CONFIRM (link is external) GENTOO
extraputty -- extraputty	The TFTP server in ExtraPuTTY 0.30 and earlier allows remote attackers to cause a denial of service (crash) via a large (1) read or (2) write TFTP protocol message.	2017-03-27	5.0	CVE-2017-7183 MISC (link is external) BUGTRAQ (link is external) BID (link is external)
f5 -- big-ip_webaccelerator	The Traffic Management Microkernel (TMM) in F5 BIG-IP before 11.5.4 HF3, 11.6.x before 11.6.1 HF2	2017-03-27	5.0	CVE-2016-9252 CONFIRM (link

	and 12.x before 12.1.2 does not properly handle minimum path MTU options for IPv6, which allows remote attackers to cause a denial-of-service (DoS) through unspecified vectors.			is external)
fedoraproject -- fedora	regexp.c in Artifex Software, Inc. MuJS allows attackers to cause a denial of service (NULL pointer dereference and crash) via vectors related to regular expression compilation.	2017-03-24	5.0	CVE-2016-10132 CONFIRM (link is external) MLIST (link is external) MLIST (link is external) CONFIRM (link is external) FEDORA
fedoraproject -- fedora	The bmp_getdata function in libjasper/bmp/bmp_dec.c in JasPer 1.900.5 allows remote attackers to cause a denial of service (NULL pointer dereference) by calling the imginfo command with a crafted BMP image. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8690.	2017-03-28	4.3	CVE-2016-8884 MLIST (link is external) MLIST (link is external) BID (link is external) MISC CONFIRM (link is external) CONFIRM (link is external) FEDORA FEDORA
fedoraproject -- fedora	ark before 16.12.1 might allow remote attackers to execute arbitrary code via an executable in an archive, related to associated applications.	2017-03-27	6.8	CVE-2017-5330 MLIST (link is external) BID (link is external) CONFIRM CONFIRM FEDORA GENTOO
firebirdsql -- firebird	Insufficient checks in the UDF subsystem in Firebird 2.5.x before 2.5.7 and 3.0.x before 3.0.2 allow remote authenticated users to execute code by using a 'system' entrypoint from fbudf.so.	2017-03-24	6.5	CVE-2017-6369 CONFIRM BID (link is external)
fomori -- cherrymusic	Directory traversal vulnerability in Cherry Music before 0.36.0 allows remote authenticated users to read arbitrary files via the "value" parameter to "download."	2017-03-27	4.0	CVE-2015-8309 CONFIRM BID (link is external) CONFIRM (link

				is external) CONFIRM (link is external) EXPLOIT-DB (link is external)
freeradius -- freeradius	The EAP-PWD module in FreeRADIUS 3.0 through 3.0.8 allows remote attackers to cause a denial of service (NULL pointer dereference and server crash) via a zero-length EAP-PWD packet.	2017-03-27	4.3	CVE-2015-8762 CONFIRM MLIST (link is external)
freeradius -- freeradius	The EAP-PWD module in FreeRADIUS 3.0 through 3.0.8 allows remote attackers to have unspecified impact via a crafted (1) commit or (2) confirm message, which triggers an out-of-bounds read.	2017-03-27	6.8	CVE-2015-8763 CONFIRM MLIST (link is external)
freeradius -- freeradius	Off-by-one error in the EAP-PWD module in FreeRADIUS 3.0 through 3.0.8, which triggers a buffer overflow.	2017-03-27	6.8	CVE-2015-8764 CONFIRM MLIST (link is external)
getsymphony -- symphony_cms	Symphony 2.6.9 has XSS in publish/notes/edit/##/saved/ via the bottom form field.	2017-03-26	4.3	CVE-2017-6067 BID (link is external) MISC (link is external)
gnu -- bash	The path autocompletion feature in Bash 4.4 allows local users to gain privileges via a crafted filename starting with a " (double quote) character and a command substitution metacharacter.	2017-03-27	4.6	CVE-2017-5932 CONFIRM MLIST (link is external) BID (link is external) MLIST
gnu -- binutils	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has an invalid read (of size 8) because the code to emit relocs (bfd_elf_final_link function in bfd/elflink.c) does not check the format of the input file before trying to read the ELF reloc section header. The vulnerability leads to a GNU linker (ld) program crash.	2017-03-29	4.3	CVE-2017-7299 BID (link is external) CONFIRM
gnu -- binutils	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has an aout_link_add_symbols function in bfd/aoutx.h that is vulnerable to a heap-based buffer over-read (off-by-one) because of an incomplete check for invalid string offsets while loading symbols, leading	2017-03-29	5.0	CVE-2017-7300 BID (link is external) CONFIRM

	to a GNU linker (ld) program crash.			
gnu -- binutils	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has an aout_link_add_symbols function in bfd/aoutx.h that has an off-by-one vulnerability because it does not carefully check the string offset. The vulnerability could lead to a GNU linker (ld) program crash.	2017-03-29	5.0	CVE-2017-7301 BID (link is external) CONFIRM
gnu -- binutils	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has a swap_std_reloc_out function in bfd/aoutx.h that is vulnerable to an invalid read (of size 4) because of missing checks for relocs that could not be recognised. This vulnerability causes Binutils utilities like strip to crash.	2017-03-29	5.0	CVE-2017-7302 BID (link is external) CONFIRM
gnu -- binutils	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read (of size 4) because of missing a check (in the find_link function) for null headers before attempting to match them. This vulnerability causes Binutils utilities like strip to crash.	2017-03-29	5.0	CVE-2017-7303 BID (link is external) CONFIRM
gnu -- binutils	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read (of size 8) because of missing a check (in the copy_special_section_fields function) for an invalid sh_link field before attempting to follow it. This vulnerability causes Binutils utilities like strip to crash.	2017-03-29	5.0	CVE-2017-7304 BID (link is external) CONFIRM
gnu -- gnutls	The stream reading functions in lib/opencdk/read-packet.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to cause a denial of service (out-of-memory error and crash) via a crafted OpenPGP certificate.	2017-03-24	5.0	CVE-2017-5335 SUSE MLIST (link is external) MLIST (link is external) BID (link is external) SECTRACK (link is external) MISC CONFIRM (link is external) CONFIRM

				GENTOO
go-jose_project -- go-jose	go-jose before 1.0.4 suffers from an invalid curve attack for the ECDH-ES algorithm. When deriving a shared key using ECDH-ES for an encrypted message, go-jose neglected to check that the received public key on a message is on the same curve as the static private key of the receiver, thus making it vulnerable to an invalid curve attack.	2017-03-27	6.4	CVE-2016-9121 MISC (link is external) MISC (link is external) MISC (link is external)
go-jose_project -- go-jose	go-jose before 1.0.4 suffers from multiple signatures exploitation. The go-jose library supports messages with multiple signatures. However, when validating a signed message the API did not indicate which signature was valid, which could potentially lead to confusion. For example, users of the library might mistakenly read protected header values from an attached signature that was different from the one originally validated.	2017-03-27	5.0	CVE-2016-9122 MISC (link is external) MISC (link is external) MISC (link is external)
go-jose_project -- go-jose	go-jose before 1.0.5 suffers from a CBC-HMAC integer overflow on 32-bit architectures. An integer overflow could lead to authentication bypass for CBC-HMAC encrypted ciphertexts on 32-bit architectures.	2017-03-27	5.0	CVE-2016-9123 MISC (link is external) MISC (link is external) MISC (link is external)
ibm -- cognos_business_intelligence	IBM Cognos Business Intelligence 10.2 could allow a user with lower privilege Capabilities to adopt the Capabilities of a higher-privilege user by intercepting the higher-privilege user's cookie value from its HTTP request and then reusing it in subsequent requests. IBM Reference #: 1993718.	2017-03-27	6.5	CVE-2016-8960 CONFIRM (link is external) BID (link is external)
ibm -- kenexa_lcms_premier	IBM Kenexa LCMS Premier on Cloud 9.x and 10.0 could allow a remote attacker to obtain sensitive information, caused by the failure to set the secure flag for the session cookie in SSL mode. By intercepting its transmission within an HTTP session, an attacker could exploit this vulnerability to capture the cookie and obtain sensitive information. IBM Reference #: 1998874.	2017-03-27	4.0	CVE-2017-1142 CONFIRM (link is external) BID (link is external)
ibm --	IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 stores	2017-03-27	4.3	CVE-2016-6102

security_key_lifecycle_manager	sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM Reference #: 2000359.			CONFIRM (link is external) BID (link is external)
ibm -- tririga_application_platform	IBM TRIRIGA Report Manager 3.2 through 3.5 contains a vulnerability that could allow an authenticated user to execute actions that they do not have access to. IBM Reference #: 1999563.	2017-03-27	6.5	CVE-2017-1153 CONFIRM (link is external) BID (link is external)
ibm -- websphere_portal	IBM WebSphere Portal 8.5 and 9.0 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 #: 2000152.	2017-03-27	4.3	CVE-2017-1120 CONFIRM (link is external) BID (link is external)
imagemagick -- imagemagick	Double free vulnerability in magick/profile.c in ImageMagick allows remote attackers to have unspecified impact via a crafted file.	2017-03-24	6.8	CVE-2017-5506 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	Heap-based buffer overflow in the PushQuantumPixel function in ImageMagick before 6.9.7-3 and 7.x before 7.0.4-3 allows remote attackers to cause a denial of service (application crash) via a crafted TIFF file.	2017-03-24	4.3	CVE-2017-5508 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM
imagemagick -- imagemagick	coders/psd.c in ImageMagick allows remote attackers to have unspecified impact via a crafted PSD file, which triggers an out-of-bounds write.	2017-03-24	6.8	CVE-2017-5509 MLIST (link is external)

				MLIST (link is external) BID (link is external) CONFIRM CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	coders/psd.c in ImageMagick allows remote attackers to have unspecified impact via a crafted PSD file, which triggers an out-of-bounds write.	2017-03-24	6.8	CVE-2017-5510 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers to cause a denial of service (attempted large memory allocation and application crash) via a crafted file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8862 and CVE-2016-8866.	2017-03-27	4.3	CVE-2017-7275 BID (link is external) MISC MISC (link is external)
intelliants -- subrion_cms	Subrion CMS 4.0.5.10 has CSRF in admin/blog/add/. The attacker can add any blog entry, and can optionally insert XSS into that entry via the body parameter.	2017-03-26	6.8	CVE-2017-6002 MISC (link is external)
intelliants -- subrion_cms	Subrion CMS 4.0.5 has CSRF in admin/languages/edit/1/. The attacker can perform any Edit Language action, and can optionally insert XSS via the title parameter.	2017-03-26	6.8	CVE-2017-6066 BID (link is external) MISC (link is external)
intelliants -- subrion_cms	Subrion CMS 4.0.5 has CSRF in admin/blocks/add/. The attacker can create any block, and can optionally insert XSS via the content parameter.	2017-03-26	6.8	CVE-2017-6068 BID (link is external) MISC (link is external)

intelliants -- subrion_cms	Subrion CMS 4.0.5 has CSRF in admin/blog/add/. The attacker can add any tag, and can optionally insert XSS via the tags parameter.	2017-03-26	6.8	CVE-2017-6069 BID (link is external) MISC (link is external)
libgit2_project -- libgit2	The Git Smart Protocol support in libgit2 before 0.24.6 and 0.25.x before 0.25.1 allows remote attackers to cause a denial of service (NULL pointer dereference) via an empty packet line.	2017-03-24	5.0	CVE-2016-10129 SUSE SUSE SUSE MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
libgit2_project -- libgit2	The http_connect function in transports/http.c in libgit2 before 0.24.6 and 0.25.x before 0.25.1 might allow man-in-the-middle attackers to spoof servers by leveraging clobbering of the error variable.	2017-03-24	4.3	CVE-2016-10130 SUSE SUSE SUSE MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
libtiff -- libtiff	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted TIFF image, related to libtiff/tif_read.c:351:22.	2017-03-24	4.3	CVE-2016-10266 BID (link is external) MISC MISC (link is external)
libtiff -- libtiff	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted TIFF image, related	2017-03-24	4.3	CVE-2016-10267 BID (link is external)

	to libtiff/tif_ojpeg.c:816:8.			MISC MISC (link is external)
libtiff -- libtiff	tools/tiffcp.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (integer underflow and heap-based buffer under-read) or possibly have unspecified other impact via a crafted TIFF image, related to "READ of size 78490" and libtiff/tif_unix.c:115:23.	2017-03-24	6.8	CVE-2016-10268 BID (link is external) MISC MISC (link is external)
libtiff -- libtiff	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted TIFF image, related to "READ of size 512" and libtiff/tif_unix.c:340:2.	2017-03-24	6.8	CVE-2016-10269 BID (link is external) MISC MISC (link is external)
libtiff -- libtiff	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted TIFF image, related to "READ of size 8" and libtiff/tif_read.c:523:22.	2017-03-24	6.8	CVE-2016-10270 BID (link is external) MISC MISC (link is external)
libtiff -- libtiff	tools/tiffcrop.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (heap-based buffer over-read and buffer overflow) or possibly have unspecified other impact via a crafted TIFF image, related to "READ of size 1" and libtiff/tif_fax3.c:413:13.	2017-03-24	6.8	CVE-2016-10271 BID (link is external) MISC MISC (link is external)
libtiff -- libtiff	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted TIFF image, related to "WRITE of size 2048" and libtiff/tif_next.c:64:9.	2017-03-24	6.8	CVE-2016-10272 BID (link is external) MISC MISC (link is external)
linux -- linux_kernel	The vmw_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.5 does not check for a zero value of certain levels data, which allows local users to cause a denial of service (ZERO_SIZE_PTR dereference, and GPF and possibly panic) via a crafted ioctl call for a /dev/dri/renderD* device.	2017-03-24	4.9	CVE-2017-7261 MISC (link is external) BID (link is external) MISC (link is external) MISC

linux -- linux_kernel	The TCP stack in the Linux kernel through 4.10.6 mishandles the SCM_TIMESTAMPING_OPT_STATS feature, which allows local users to obtain sensitive information from the kernel's internal socket data structures or cause a denial of service (out-of-bounds read) via crafted system calls, related to net/core/skbuff.c and net/socket.c.	2017-03-28	6.6	CVE-2017-7277 CONFIRM CONFIRM BID (link is external) CONFIRM (link is external) CONFIRM (link is external) MISC CONFIRM CONFIRM
miele_professional -- pst10_webserver	An issue was discovered on Miele Professional PG 8528 PST10 devices. The corresponding embedded webserver "PST10 WebServer" typically listens to port 80 and is prone to a directory traversal attack; therefore, an unauthenticated attacker may be able to exploit this issue to access sensitive information to aide in subsequent attacks. A Proof of Concept is GET /../../../../../../../../../../../etc/shadow HTTP/1.1.	2017-03-24	5.0	CVE-2017-7240 MISC BID (link is external)
modx -- modx_revolution	setup/controllers/language.php in MODX Revolution 2.5.4-pl and earlier does not properly constrain the language parameter, which allows remote attackers to conduct Cookie-Bombing attacks and cause a denial of service (cookie quota exhaustion), or conduct HTTP Response Splitting attacks with resultant XSS, via an invalid parameter value.	2017-03-30	4.3	CVE-2017-7320 BID (link is external) MISC (link is external)
modx -- modx_revolution	The (1) update and (2) package-installation features in MODX Revolution 2.5.4-pl and earlier do not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and trigger the execution of arbitrary code via a crafted certificate.	2017-03-30	6.8	CVE-2017-7322 BID (link is external) MISC (link is external)
modx -- modx_revolution	The (1) update and (2) package-installation features in MODX Revolution 2.5.4-pl and earlier use http://rest.modx.com by default, which allows man-in-the-middle attackers to spoof servers and trigger the execution of arbitrary code by leveraging the lack of the HTTPS protection mechanism.	2017-03-30	6.8	CVE-2017-7323 BID (link is external) MISC (link is external)
moodle -- moodle	In Moodle 3.2.x, global search displays user names	2017-03-26	5.0	CVE-2017-2643 BID (link is

	for unauthenticated users.			external) CONFIRM
moodle -- moodle	In Moodle 3.x, XSS can occur via evidence of prior learning.	2017-03-26	4.3	CVE-2017-2644 BID (link is external) CONFIRM
moodle -- moodle	In Moodle 3.x, XSS can occur via attachments to evidence of prior learning.	2017-03-26	4.3	CVE-2017-2645 BID (link is external) CONFIRM
netflix -- security_monkey	Netflix Security Monkey before 0.8.0 has an Open Redirect. The logout functionality accepted the "next" parameter which then redirects to any domain irrespective of the Host header.	2017-03-26	5.8	CVE-2017-7266 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
nextcloud -- nextcloud	Nextcloud Server before 9.0.52 & ownCloud Server before 9.0.4 are vulnerable to a content-spoofing attack in the files app. The location bar in the files app was not verifying the passed parameters. An attacker could craft an invalid link to a fake directory structure and use this to display an attacker-controlled error message to the user.	2017-03-27	5.0	CVE-2016-9460 MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC
nextcloud -- nextcloud	Nextcloud Server before 9.0.54 and 10.0.0 suffers from an improper authorization check on removing shares. The Sharing Backend as implemented in Nextcloud does differentiate between shares to users and groups. In case of a received group share, users should be able to unshare the file to themselves but not to the whole group. The previous API implementation simply unshared the file to all users in the group.	2017-03-27	4.0	CVE-2016-9464 MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external)
nextcloud -- nextcloud	Nextcloud Server before 9.0.54 and 10.0.1 & ownCloud Server before 9.0.6 and 9.1.2 suffer from content spoofing in the files app. The location bar in	2017-03-27	5.0	CVE-2016-9467 MISC (link is external)

	the files app was not verifying the passed parameters. An attacker could craft an invalid link to a fake directory structure and use this to display an attacker-controlled error message to the user.			MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC
nextcloud -- nextcloud	Nextcloud Server before 9.0.54 and 10.0.1 & ownCloud Server before 9.0.6 and 9.1.2 suffer from content spoofing in the dav app. The exception message displayed on the DAV endpoints contained partially user-controllable input leading to a potential misrepresentation of information.	2017-03-27	5.0	CVE-2016-9468 MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC
ntp -- ntp	The mx4200_send function in the legacy MX4200 refclock in NTP before 4.2.8p10 and 4.3.x before 4.3.94 does not properly handle the return value of the snprintf function, which allows local users to execute arbitrary code via unspecified vectors, which trigger an out-of-bounds memory write.	2017-03-27	4.6	CVE-2017-6451 CONFIRM CONFIRM BID (link is external) SECTRACK (link is external)
ntp -- ntp	Stack-based buffer overflow in the Windows installer for NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows local users to have unspecified impact via an application path on the command line.	2017-03-27	4.6	CVE-2017-6452 CONFIRM CONFIRM BID (link is external) SECTRACK (link is external)
ntp -- ntp	NTP before 4.2.8p10 and 4.3.x before 4.3.94, when using PPSAPI, allows local users to gain privileges	2017-03-27	4.4	CVE-2017-6455 CONFIRM

	via a DLL in the PPSAPI_DLLS environment variable.			CONFIRM BID (link is external) SECTRACK (link is external)
ntp -- ntp	Multiple buffer overflows in the ctl_put* functions in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allow remote authenticated users to have unspecified impact via a long variable.	2017-03-27	6.5	CVE-2017-6458 CONFIRM CONFIRM BID (link is external) SECTRACK (link is external)
ntp -- ntp	Stack-based buffer overflow in the reslist function in ntpq in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote servers have unspecified impact via a long flagstr variable in a restriction list response.	2017-03-27	6.5	CVE-2017-6460 CONFIRM CONFIRM BID (link is external) SECTRACK (link is external)
ntp -- ntp	Buffer overflow in the legacy Datum Programmable Time Server (DPTS) refclock driver in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows local users to have unspecified impact via a crafted /dev/datum device.	2017-03-27	4.6	CVE-2017-6462 CONFIRM CONFIRM BID (link is external) SECTRACK (link is external)
ntp -- ntp	NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote authenticated users to cause a denial of service (daemon crash) via an invalid setting in a :config directive, related to the unpeer option.	2017-03-27	4.0	CVE-2017-6463 CONFIRM CONFIRM BID (link is external) SECTRACK (link is external)
ntp -- ntp	NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote attackers to cause a denial of service (ntpd crash) via a malformed mode configuration directive.	2017-03-27	4.0	CVE-2017-6464 CONFIRM CONFIRM BID (link is external) SECTRACK (link is external)
nuxeo -- nuxeo	Directory traversal vulnerability in the file import feature in Nuxeo Platform 6.0, 7.1, 7.2, and 7.3 allows remote authenticated users to upload and execute arbitrary JSP code via a .. (dot dot) in the X-File-Name header.	2017-03-24	6.5	CVE-2017-5869 MLIST (link is external) BID (link is external)
openslp -- openslp	The _xrealloc function in xlsp_xmalloc.c in OpenSLP 2.0.0 allows remote attackers to cause a denial of	2017-03-27	5.0	CVE-2016-4912 MLIST (link is external)

	service (NULL pointer dereference and crash) via a large number of crafted packets, which triggers a memory allocation failure.			SECTRACK (link is external) CONFIRM (link is external)
opensuse_project -- leap	Cross-site scripting (XSS) vulnerability in the Classic-UI with the CSV export link and pagination feature in Icinga before 1.14 allows remote attackers to inject arbitrary web script or HTML via the query string to cgi-bin/status.cgi.	2017-03-27	4.3	CVE-2015-8010 SUSE MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
owncloud -- owncloud	Nextcloud Server before 9.0.52 & ownCloud Server before 9.0.4 are vulnerable to a log pollution vulnerability potentially leading to a local XSS. The download log functionality in the admin screen is delivering the log in JSON format to the end-user. The file was delivered with an attachment disposition forcing the browser to download the document. However, Firefox running on Microsoft Windows would offer the user to open the data in the browser as an HTML document. Thus any injected data in the log would be executed.	2017-03-27	4.3	CVE-2016-9459 MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC
owncloud -- owncloud	Nextcloud Server before 9.0.52 & ownCloud Server before 9.0.4 are not properly verifying edit check permissions on WebDAV copy actions. The WebDAV endpoint was not properly checking the permission on a WebDAV COPY action. This allowed an authenticated attacker with access to a read-only share to put new files in there. It was not possible to modify existing files.	2017-03-27	4.0	CVE-2016-9461 MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC
owncloud -- owncloud	Nextcloud Server before 9.0.52 & ownCloud Server before 9.0.4 are not properly verifying restore privileges when restoring a file. The restore capability of Nextcloud/ownCloud was not verifying whether a user has only read-only access to a share.	2017-03-27	4.0	CVE-2016-9462 MISC (link is external) MISC (link is external) MISC (link is

	Thus a user with read-only access was able to restore old versions.			external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC
owncloud -- owncloud	Nextcloud Server before 9.0.54 and 10.0.1 & ownCloud Server before 9.1.2, 9.0.6, and 8.2.9 suffer from SMB User Authentication Bypass. Nextcloud/ownCloud include an optional and not by default enabled SMB authentication component that allows authenticating users against an SMB server. This backend is implemented in a way that tries to connect to a SMB server and if that succeeded consider the user logged-in. The backend did not properly take into account SMB servers that have any kind of anonymous auth configured. This is the default on SMB servers nowadays and allows an unauthenticated attacker to gain access to an account without valid credentials. Note: The SMB backend is disabled by default and requires manual configuration in the Nextcloud/ownCloud config file. If you have not configured the SMB backend then you're not affected by this vulnerability.	2017-03-27	6.8	CVE-2016-9463 MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC MISC (link is external)
owncloud -- owncloud	Nextcloud Server before 10.0.1 & ownCloud Server before 9.0.6 and 9.1.2 suffer from Reflected XSS in the Gallery application. The gallery app was not properly sanitizing exception messages from the Nextcloud/ownCloud server. Due to an endpoint where an attacker could influence the error message, this led to a reflected Cross-Site-Scripting vulnerability.	2017-03-27	4.3	CVE-2016-9466 MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC
php -- php	PHP through 7.1.3 enables potential SSRF in applications that accept an fsockopen hostname argument with an expectation that the port	2017-03-27	5.8	CVE-2017-7272 BID (link is external) CONFIRM (link

	number is constrained. Because a :port syntax is recognized, fsockopen will use the port number that is specified in the hostname argument, instead of the port number in the second argument of the function.			is external) CONFIRM (link is external)
potrace_project -- potrace	The bm_readbody_bmp function in bitmap_io.c in Potrace 1.14 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted BMP image. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8698.	2017-03-26	6.8	CVE-2017-7263 BID (link is external) MISC
radare -- radare2	The r_pkcs7_parse_cms function in libr/util/r_pkcs7.c in radare2 1.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted PE file.	2017-03-27	4.3	CVE-2017-7274 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
revive-adserver -- revive_adserver	Revive Adserver before 3.2.3 suffers from Improper Restriction of Excessive Authentication Attempts. The login page of Revive Adserver is vulnerable to password-guessing attacks. An account lockdown feature was considered, but rejected to avoid introducing service disruptions to regular users during such attacks. A random delay has instead been introduced as a countermeasure in case of password failures, along with a system to discourage parallel brute forcing. These systems will effectively allow the valid users to log in to the adserver, even while an attack is in progress.	2017-03-27	5.0	CVE-2016-9124 MISC (link is external) MISC (link is external) MISC (link is external)
revive-adserver -- revive_adserver	Revive Adserver before 3.2.3 suffers from Cross-Site Request Forgery (CSRF). The password recovery form in Revive Adserver is vulnerable to CSRF attacks. This vulnerability could be exploited to send a large number of password recovery emails to the registered users, especially in conjunction with a bug that caused recovery emails to be sent to all the users at once. Both issues have been fixed.	2017-03-27	6.8	CVE-2016-9127 MISC (link is external) MISC (link is external) MISC (link is external)
revive-adserver --	Revive Adserver before 3.2.3 suffers from	2017-03-27	5.0	CVE-2016-9129

revive_adserver	Information Exposure Through Discrepancy. It is possible to check whether or not an email address was associated to one or more user accounts on a target Revive Adserver instance by examining the message printed by the password recovery system. Such information cannot however be used directly to log in to the system, which requires a username.			MISC (link is external) MISC (link is external) MISC (link is external)
revive-adserver -- revive_adserver	Revive Adserver before 3.2.3 suffers from Cross-Site Request Forgery (CSRF). A number of scripts in Revive Adserver's user interface are vulnerable to CSRF attacks: `www/admin/banner-acl.php`, `www/admin/banner-activate.php`, `www/admin/banner-advanced.php`, `www/admin/banner-modify.php`, `www/admin/banner-swf.php`, `www/admin/banner-zone.php`, `www/admin/tracker-modify.php`.	2017-03-27	6.8	CVE-2016-9455 BID (link is external) MISC (link is external) MISC (link is external) MISC (link is external)
revive-adserver -- revive_adserver	Revive Adserver before 3.2.3 suffers from Cross-Site Request Forgery (CSRF). The Revive Adserver team conducted a security audit of the admin interface scripts in order to identify and fix other potential CSRF vulnerabilities. Over 20+ such issues were fixed.	2017-03-27	6.8	CVE-2016-9456 BID (link is external) MISC (link is external) MISC (link is external)
s-nail_project -- s-nail	Directory traversal vulnerability in the setuid root helper binary in S-nail (later S-mailx) before 14.8.16 allows local users to write to arbitrary files and consequently gain root privileges via a .. (dot dot) in the randstr argument.	2017-03-27	6.9	CVE-2017-5899 MLIST (link is external) MLIST (link is external) BID (link is external) MLIST (link is external)
siemens -- ruggedcom_rox_i	Siemens RUGGEDCOM ROX I (all versions) contain a vulnerability that could allow an authenticated user to read arbitrary files through the web interface at port 10000/TCP and access sensitive information.	2017-03-28	4.0	CVE-2017-2686 BID (link is external) CONFIRM (link is external)
siemens -- ruggedcom_rox_i	Siemens RUGGEDCOM ROX I (all versions) contain a vulnerability in the integrated web server at port 10000/TCP which is prone to reflected Cross-Site Scripting attacks if an unsuspecting user is induced	2017-03-28	4.3	CVE-2017-2687 BID (link is external) CONFIRM (link is external)

	to click on a malicious link.			
siemens -- ruggedcom_rox_i	The integrated web server in Siemens RUGGEDCOM ROX I (all versions) at port 10000/TCP could allow remote attackers to perform actions with the privileges of an authenticated user, provided the targeted user has an active session and is induced into clicking on a malicious link or into visiting a malicious website, aka CSRF.	2017-03-28	6.8	CVE-2017-2688 BID (link is external) CONFIRM (link is external)
siemens -- ruggedcom_rox_i	Siemens RUGGEDCOM ROX I (all versions) allow an authenticated user to bypass access restrictions in the web interface at port 10000/TCP to obtain privileged file system access or change configuration settings.	2017-03-28	6.5	CVE-2017-2689 BID (link is external) CONFIRM (link is external)
solarwinds -- log_and_event_manager	The editbanner feature in SolarWinds LEM (aka SIEM) through 6.3.1 allows remote authenticated users to execute arbitrary code by editing /usr/local/contego/scripts/mgrconfig.pl.	2017-03-24	6.5	CVE-2017-5199 MISC (link is external) BID (link is external)
uclibc-ng_project -- uclibc-ng	The __decode_dotted function in libc/inet/resolv.c in uClibc-ng before 1.0.12 allows remote DNS servers to cause a denial of service (infinite loop) via vectors involving compressed items in a reply.	2017-03-24	5.0	CVE-2016-2224 CONFIRM (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM
uclibc-ng_project -- uclibc-ng	The __read_etc_hosts_r function in libc/inet/resolv.c in uClibc-ng before 1.0.12 allows remote DNS servers to cause a denial of service (infinite loop) via a crafted packet.	2017-03-24	5.0	CVE-2016-2225 CONFIRM (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM
yii_software -- yii	Reflected Cross-site scripting (XSS) vulnerability in Yii Framework before 2.0.11, when development mode is used, allows remote attackers to inject arbitrary web script or HTML via crafted request data that is mishandled on the debug-mode exception screen.	2017-03-27	4.3	CVE-2017-7271 BID (link is external) CONFIRM (link is external)

Low Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
cmsmadesimple -- cms_made_simple	XSS exists in the CMS Made Simple (CMSMS) 2.1.6 "Content-->News-->Add Article" feature via the m1_title parameter. Someone must login to conduct the attack.	2017-03-24	3.5	CVE-2017-7255 MISC (link is external)
cmsmadesimple -- cms_made_simple	XSS exists in the CMS Made Simple (CMSMS) 2.1.6 "Content-->News-->Add Article" feature via the m1_summary parameter. Someone must login to conduct the attack.	2017-03-24	3.5	CVE-2017-7256 MISC (link is external) BID (link is external)
cmsmadesimple -- cms_made_simple	XSS exists in the CMS Made Simple (CMSMS) 2.1.6 "Content-->News-->Add Article" feature via the m1_content parameter. Someone must login to conduct the attack.	2017-03-24	3.5	CVE-2017-7257 MISC (link is external) BID (link is external)
f5 -- big-ip_webaccelerator	In some cases the MCPD binary cache in F5 BIG-IP devices may allow a user with Advanced Shell access, or privileges to generate a qkview, to temporarily obtain normally unrecoverable information.	2017-03-27	2.1	CVE-2016-7474 BID (link is external) CONFIRM (link is external)
fomori -- cherrymusic	Cross-site scripting (XSS) vulnerability in Cherry Music before 0.36.0 allows remote authenticated users to inject arbitrary web script or HTML via the playlistname field when creating a new playlist.	2017-03-27	3.5	CVE-2015-8310 CONFIRM BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
ibm -- call_center_for_commerce	IBM Call Center for Commerce 9.3 and 9.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality	2017-03-27	3.5	CVE-2016-6056 CONFIRM (link is external) BID (link is external)

	potentially leading to credentials disclosure within a trusted session. IBM Reference #: 2000442.			
ibm -- kenexa_lcms_premier	IBM Kenexa LCMS Premier on Cloud 9.x and 10.0 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM Reference #: 1998874.	2017-03-27	3.5	CVE-2017-1143 CONFIRM (link is external) BID (link is external)
ibm -- tririga_application_platform	IBM TRIRIGA 3.3, 3.4, and 3.5 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 #: 1996200.	2017-03-27	3.5	CVE-2016-9737 CONFIRM (link is external) BID (link is external)
metinfo -- metinfo	Cross-site scripting (XSS) vulnerability in MetInfo 5.3.15 allows remote authenticated users to inject arbitrary web script or HTML via the name_2 parameter to admin/column/delete.php.	2017-03-27	3.5	CVE-2017-6878 MISC (link is external) FULLDISC BID (link is external)
miniupnp_project -- minisspd	The processRequest function in minissdpd.c in MiniSSDPd 1.2.20130907-3 allows local users to cause a denial of service (out-of-bounds memory access and daemon crash) via vectors involving a negative length value.	2017-03-24	2.1	CVE-2016-3178 MISC (link is external) MLIST (link is external) CONFIRM CONFIRM (link is external)
miniupnp_project -- minisspd	The processRequest function in minissdpd.c in MiniSSDPd 1.2.20130907-3 allows local users to cause a denial of service (invalid free and daemon crash) via vectors related to error handling.	2017-03-24	2.1	CVE-2016-3179 MISC (link is external) MLIST (link is external) CONFIRM CONFIRM (link is external)
moodle -- moodle	In Moodle 3.2.2+, there is XSS in the Course summary filter of the "Add a new course" page, as demonstrated by a crafted attribute of an SVG element.	2017-03-29	3.5	CVE-2017-7298 MISC (link is external) BID (link is external)
netcomm -- nb16wv-	Cross-site scripting (XSS) vulnerability in the NetComm NB16WV-02 router with firmware	2017-03-29	3.5	CVE-2017-5900 FULLDISC

02_firmware	NB16WV_R0.09 allows remote authenticated users to inject arbitrary web script or HTML via the S801F0334 parameter to hdd.htm.			BID (link is external)
nextcloud -- nextcloud	Nextcloud Server before 10.0.1 & ownCloud Server before 9.0.6 and 9.1.2 suffer from Stored XSS in CardDAV image export. The CardDAV image export functionality as implemented in Nextcloud/ownCloud allows the download of images stored within a vCard. Due to not performing any kind of verification on the image content this is prone to a stored Cross-Site Scripting attack.	2017-03-27	3.5	CVE-2016-9465 MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external) MISC
ntp -- ntp	The Windows installer for NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows local users to have unspecified impact via vectors related to an argument with multiple null bytes.	2017-03-27	2.1	CVE-2017-6459 CONFIRM CONFIRM BID (link is external) SECTRACK (link is external)
oneplus -- oxygenos	With OxygenOS before 4.0.3, when a charger is connected to a powered-off OnePlus 3 or 3T device, the platform starts with adbd enabled. Therefore, a malicious charger or a physical attacker can open up, without authorization, an ADB session with the device, in order to further exploit other vulnerabilities and/or exfiltrate sensitive information.	2017-03-26	3.6	CVE-2017-5622 BID (link is external) MISC (link is external)
qemu -- qemu	The cirrus_do_copy function in hw/display/cirrus_vga.c in QEMU (aka Quick Emulator), when cirrus graphics mode is VGA, allows local guest OS privileged users to cause a denial of service (divide-by-zero error and QEMU process crash) via vectors involving blit pitch values.	2017-03-27	2.1	CVE-2016-9922 CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external) MLIST
qemu -- qemu	The xhci_kick_epctx function in hw/usb/hcd-xhci.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (infinite loop and QEMU process crash) via vectors related to control transfer descriptor sequence.	2017-03-27	2.1	CVE-2017-5973 CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external)

				MLIST
revive-adserver -- revive_adserver	Revive Adserver before 3.2.3 suffers from persistent XSS. Usernames are not properly escaped when displayed in the audit trail widget of the dashboard upon login, allowing persistent XSS attacks. An authenticated user with enough privileges to create other users could exploit the vulnerability to access the administrator account.	2017-03-27	3.5	CVE-2016-9126 MISC (link is external) MISC (link is external) MISC (link is external)
revive-adserver -- revive_adserver	Revive Adserver before 3.2.3 suffers from reflected XSS. The affiliate-preview.php script in www/admin is vulnerable to a reflected XSS attack. This vulnerability could be used by an attacker to steal the session ID of an authenticated user, by tricking them into visiting a specifically crafted URL.	2017-03-27	3.5	CVE-2016-9128 MISC (link is external) MISC (link is external) MISC (link is external) MISC (link is external)
revive-adserver -- revive_adserver	Revive Adserver before 3.2.3 suffers from Persistent XSS. A vector for persistent XSS attacks via the Revive Adserver user interface exists, requiring a trusted (non-admin) account. The website name wasn't properly escaped when displayed in the campaign-zone.php script.	2017-03-27	3.5	CVE-2016-9130 MISC (link is external) MISC (link is external)
revive-adserver -- revive_adserver	Revive Adserver before 3.2.3 suffers from Persistent XSS. A vector for persistent XSS attacks via the Revive Adserver user interface exists, requiring a trusted (non-admin) account. The banner image URL for external banners wasn't properly escaped when displayed in most of the banner related pages.	2017-03-27	3.5	CVE-2016-9454 BID (link is external) MISC (link is external) MISC (link is external)
revive-adserver -- revive_adserver	Revive Adserver before 3.2.3 suffers from Reflected XSS. `www/admin/stats.php` is vulnerable to reflected XSS attacks via multiple parameters that are not properly sanitised or escaped when displayed, such as setPerPage, pageId, bannerid, period_start, period_end, and possibly others.	2017-03-27	3.5	CVE-2016-9457 BID (link is external) MISC (link is external) MISC (link is external) MISC (link is external)
revive-adserver -- revive_adserver	Revive Adserver before 3.2.5 and 4.0.0 suffers from Special Element Injection. Usernames weren't properly sanitised when creating users on a Revive Adserver instance. Especially, control characters	2017-03-27	2.1	CVE-2016-9471 MISC (link is external) MISC (link is external)

	were not filtered, allowing apparently identical usernames to co-exist in the system, due to the fact that such characters are normally ignored when an HTML page is displayed in a browser. The issue could have therefore been exploited for user spoofing, although elevated privileges are required to create users within Revive Adserver.			
revive-adserver -- revive_adserver	Revive Adserver before 3.2.5 and 4.0.0 suffers from Reflected XSS. The Revive Adserver web installer scripts were vulnerable to a reflected XSS attack via the dbHost, dbUser, and possibly other parameters. It has to be noted that the window for such attack vectors to be possible is extremely narrow and it is very unlikely that such an attack could be actually effective.	2017-03-27	3.5	CVE-2016-9472 MISC (link is external) MISC (link is external) MISC (link is external)
siemens -- ruggedcom_rox_i	The integrated web server in Siemens RUGGEDCOM ROX I (all versions) at port 10000/TCP could allow an authenticated user to perform stored Cross-Site Scripting attacks.	2017-03-28	3.5	CVE-2017-6864 BID (link is external) CONFIRM (link is external)

- 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).