Vulnerability Summary for the Week of February 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**
atheme -- atheme	Memory leak in the login_user function in saslserv/main.c in saslserv/main.so in Atheme 7.2.7 allows a remote unauthenticated attacker to consume memory and cause a denial of service. This is fixed in 7.2.8.	2017-03-02	7.8	CVE-2017-6384 CONFIRM (link is external) CONFIRM (link is external)
dropbear_ssh_project -- dropbear_ssh	Format string vulnerability in Dropbear SSH before 2016.74 allows remote attackers to execute arbitrary code via format string specifiers in the (1) username or (2) host argument.	2017-03-03	10.0	CVE-2016-7406 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) GENTOO
dropbear_ssh_project -- dropbear_ssh	The dropbearconvert command in Dropbear SSH before 2016.74 allows attackers to execute arbitrary code via a crafted OpenSSH key file.	2017-03-03	10.0	CVE-2016-7407 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)

				GENTOO
fedoraproject -- fedora	Multiple integer overflows in the (1) vnc_connection_server_message and (2) vnc_color_map_set functions in gtk-vnc before 0.7.0 allow remote servers to cause a denial of service (crash) or possibly execute arbitrary code via vectors involving SetColorMapEntries, which triggers a buffer overflow.	2017-02-28	7.5	CVE-2017-5885 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM FEDORA
iceni -- argus	An exploitable uninitialized variable vulnerability which leads to a stack-based buffer overflow exists in Iceni Argus. When it attempts to convert a malformed PDF to XML a stack variable will be left uninitialized which will later be used to fetch a length that is used in a copy operation. In most cases this will allow an aggressor to write outside the bounds of a stack buffer which is used to contain colors. This can lead to code execution under the context of the account running the tool.	2017-02-27	9.3	CVE-2016-8385 BID (link is external) MISC (link is external)
iceni -- argus	An exploitable heap-based buffer overflow exists in Iceni Argus. When it attempts to convert a PDF containing a malformed font to XML, the tool will attempt to use a size out of the font to search through a linked list of buffers to return. Due to a signedness issue, a buffer smaller than the requested size will be returned. Later when the tool tries to populate this buffer, the overflow will occur which can lead to code execution under the context of the user running the tool.	2017-02-27	9.3	CVE-2016-8386 BID (link is external) MISC (link is external)
iceni -- argus	An exploitable heap-based buffer overflow exists in Iceni Argus. When it attempts to convert a malformed PDF with an object encoded w/ multiple encoding types terminating with an LZW encoded type, an overflow may occur due to a lack of bounds checking by the LZW decoder. This can lead to code execution under the context of the account of the user running it.	2017-02-27	9.3	CVE-2016-8387 BID (link is external) MISC (link is external)

iceni -- argus	An exploitable arbitrary heap-overwrite vulnerability exists within Iceni Argus. When it attempts to convert a malformed PDF to XML, it will explicitly trust an index within the specific font object and use it to write the font's name to a single object within an array of objects.	2017-02-28	9.3	CVE-2016-8388 BID (link is external) MISC (link is external)
iceni -- argus	An exploitable integer-overflow vulnerability exists within Iceni Argus. When it attempts to convert a malformed PDF to XML, it will attempt to convert each character from a font into a polygon and then attempt to rasterize these shapes. As the application attempts to iterate through the rows and initializing the polygon shape in the buffer, it will write outside of the bounds of said buffer. This can lead to code execution under the context of the account running it.	2017-02-28	9.3	CVE-2016-8389 BID (link is external) MISC (link is external)
justsystems -- ichitaro	When copying filedata into a buffer, JustSystems Ichitaro Office 2016 Trial will calculate two values to determine how much data to copy from the document. If both of these values are larger than the size of the buffer, the application will choose the smaller of the two and trust it to copy data from the file. This value is larger than the buffer size, which leads to a heap-based buffer overflow. This overflow corrupts an offset in the heap used in pointer arithmetic for writing data and can lead to code execution under the context of the application.	2017-02-24	7.5	CVE-2017-2789 BID (link is external) MISC (link is external)
justsystems -- ichitaro	When processing a record type of 0x3c from a Workbook stream from an Excel file (.xls), JustSystems Ichitaro Office trusts that the size is greater than zero, subtracts one from the length, and uses this result as the size for a memcpy. This results in a heap-based buffer overflow and can lead to code execution under the context of the application.	2017-02-24	7.5	CVE-2017-2790 BID (link is external) MISC (link is external)
libdwarf_project -- libdwarf	(1) libdwarf/dwarf_leb.c and (2) dwarfdump/print_frames.c in libdwarf before	2017-02-28	7.5	CVE-2016-9558 MLIST (link is

	20161124 allow remote attackers to have unspecified impact via a crafted bit pattern in a signed leb number, aka a "negation overflow."			external) MLIST (link is external) BID (link is external) MISC CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	The ip_cmsg_recv_checksum function in net/ipv4/ip_sockglue.c in the Linux kernel before 4.10.1 has incorrect expectations about skb data layout, which allows local users to cause a denial of service (buffer over-read) or possibly have unspecified other impact via crafted system calls, as demonstrated by use of the MSG_MORE flag in conjunction with loopback UDP transmission.	2017-03-01	7.2	CVE-2017-6347 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
microsoft -- internet_explorer	Microsoft Internet Explorer 11 and Microsoft Edge have a type confusion issue in the Layout::MultiColumnBoxBuilder::HandleColumnBreakOnColumnSpanningElement function in mshtml.dll, which allows remote attackers to execute arbitrary code via vectors involving a crafted Cascading Style Sheets (CSS) token sequence and crafted JavaScript code that operates on a TH element.	2017-02-26	7.6	CVE-2017-0037 BID (link is external) MISC
plone -- plone	Plone 4.0 through 5.1a1 does not have security declarations for Dexterity content-related WebDAV requests, which allows remote attackers to gain webdav access via unspecified vectors.	2017-02-24	7.5	CVE-2016-4041 MLIST (link is external) CONFIRM
revive-adserver -- revive_adserver	Revive Adserver before 4.0.1 allows remote attackers to execute arbitrary code via serialized data in the cookies related to the delivery scripts.	2017-03-03	7.5	CVE-2017-5830 MLIST (link is external) CONFIRM (link is external)
rubyzip -- rubyzip	The Zip::File component in the rubyzip gem before 1.2.1 for Ruby has a directory traversal vulnerability. If a site allows uploading of .zip files, an attacker can upload a malicious file that	2017-02-27	7.5	CVE-2017-5946 BID (link is external) CONFIRM (link is external)

	uses "../" pathname substrings to write arbitrary files to the filesystem.			CONFIRM (link is external)
veritas -- netbackup_appliance	An issue was discovered in Veritas NetBackup Before 7.7.2 and NetBackup Appliance Before 2.7.2. Privileged remote command execution on NetBackup Server and Client (on the server or a connected client) can occur.	2017-03-02	7.2	CVE-2017-6399 CONFIRM (link is external)
veritas -- netbackup_appliance	An issue was discovered in Veritas NetBackup Before 7.7.2 and NetBackup Appliance Before 2.7.2. Privileged command execution on NetBackup Server and Client can occur (on the local system).	2017-03-02	7.2	CVE-2017-6400 CONFIRM (link is external)
veritas -- netbackup_appliance	An issue was discovered in Veritas NetBackup Before 8.0 and NetBackup Appliance Before 3.0. NetBackup Cloud Storage Service uses a hardcoded username and password.	2017-03-02	7.5	CVE-2017-6403 CONFIRM (link is external)
veritas -- netbackup_appliance	An issue was discovered in Veritas NetBackup Before 7.7.2 and NetBackup Appliance Before 2.7.2. Arbitrary privileged command execution, using whitelist directory escape with "../" substrings, can occur.	2017-03-02	7.2	CVE-2017-6406 CONFIRM (link is external)
veritas -- netbackup_appliance	An issue was discovered in Veritas NetBackup Before 7.7.2 and NetBackup Appliance Before 2.7.2. Privileged remote command execution on NetBackup Server and Client (on the server or a connected client) can occur.	2017-03-02	7.2	CVE-2017-6407 CONFIRM (link is external)
veritas -- netbackup_appliance	An issue was discovered in Veritas NetBackup 8.0 and earlier and NetBackup Appliance 3.0 and earlier. Unauthenticated CORBA interfaces permit inappropriate access.	2017-03-02	7.5	CVE-2017-6409 CONFIRM (link is external)
vim -- vim	An integer overflow at a u_read_undo memory allocation site would occur for vim before patch 8.0.0377, if it does not properly validate values for tree length when reading a corrupted undo file, which may lead to resultant buffer overflows.	2017-02-27	7.5	CVE-2017-6349 BID (link is external) MISC (link is external) MISC (link is external) MISC (link is external)

vim -- vim	An integer overflow at an unserialize_uep memory allocation site would occur for vim before patch 8.0.0378, if it does not properly validate values for tree length when reading a corrupted undo file, which may lead to resultant buffer overflows.	2017-02-27	7.5	CVE-2017-6350 BID (link is external) 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**
cisco -- netflow_generation_appliance_software	A vulnerability in the Stream Control Transmission Protocol (SCTP) decoder of the Cisco NetFlow Generation Appliance (NGA) with software before 1.1(1a) could allow an unauthenticated, remote attacker to cause the device to hang or unexpectedly reload, causing a denial of service (DoS) condition. The vulnerability is due to incomplete validation of SCTP packets being monitored on the NGA data ports. An attacker could exploit this vulnerability by sending malformed SCTP packets on a network that is monitored by an NGA data port. SCTP packets addressed to the IP address of the NGA itself will not trigger this vulnerability. An exploit could allow the attacker to cause the appliance to become unresponsive or reload, causing a DoS condition. User interaction could be needed to recover the device using the reboot command from the CLI. The following Cisco NetFlow Generation Appliances are vulnerable: NGA 3140, NGA 3240, NGA 3340. Cisco Bug IDs: CSCvc83320.	2017-03-01	5.0	CVE-2017-3826 BID (link is external) CONFIRM (link is external)

dropbear_ssh_project -- dropbear_ssh	The dbclient in Dropbear SSH before 2016.74 allows remote attackers to execute arbitrary code via a crafted (1) -m or (2) -c argument.	2017-03-03	6.5	CVE-2016-7408 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) GENTOO
fedoraproject -- fedora	Buffer overflow in the calc_coeff function in libass/ass_blur.c in libass before 0.13.4 allows remote attackers to cause a denial of service via unspecified vectors.	2017-03-03	5.0	CVE-2016-7970 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) FEDORA FEDORA FEDORA GENTOO
fedoraproject -- fedora	gtk-vnc before 0.7.0 does not properly check boundaries of subrectangle-containing tiles, which allows remote servers to execute arbitrary code via the src x, y coordinates in a crafted (1) rre, (2) hextile, or (3) copyrect tile.	2017-02-28	6.8	CVE-2017-5884 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM FEDORA
gnu -- glibc	The iconv program in the GNU C Library (aka glibc or libc6) 2.25 and earlier, when invoked with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.	2017-03-01	4.3	CVE-2016-10228 CONFIRM (link is external) BID (link is external) CONFIRM
gnu -- libiberty	Integer overflow in the string_appends function in cplus-dem.c in libiberty allows remote attackers to execute arbitrary code via a crafted executable, which triggers a buffer overflow.	2017-02-24	6.8	CVE-2016-2226 MLIST (link is external) CONFIRM
gnu -- libiberty	Use-after-free vulnerability in libiberty allows remote attackers to cause a denial of service	2017-02-24	4.3	CVE-2016-4487 MLIST (link is external)

	(segmentation fault and crash) via a crafted binary, related to "btypevec."			CONFIRM
gnu -- libiberty	Use-after-free vulnerability in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, related to "ktypevec."	2017-02-24	4.3	CVE-2016-4488 MLIST (link is external) CONFIRM
gnu -- libiberty	Integer overflow in the gnu_special function in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, related to the "demangling of virtual tables."	2017-02-24	4.3	CVE-2016-4489 MLIST (link is external) CONFIRM
gnu -- libiberty	Integer overflow in cp-demangle.c in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, related to inconsistent use of the long and int types for lengths.	2017-02-24	4.3	CVE-2016-4490 MLIST (link is external) CONFIRM
gnu -- libiberty	The d_print_comp function in cp-demangle.c in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, which triggers infinite recursion and a buffer overflow, related to a node having "itself as ancestor more than once."	2017-02-24	4.3	CVE-2016-4491 MLIST (link is external) CONFIRM MLIST
gnu -- libiberty	Buffer overflow in the do_type function in cplus-dem.c in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary.	2017-02-24	4.3	CVE-2016-4492 MLIST (link is external) CONFIRM MLIST
gnu -- libiberty	The demangle_template_value_parm and do_hpacc_template_literal functions in cplus-dem.c in libiberty allow remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted binary.	2017-02-24	4.3	CVE-2016-4493 MLIST (link is external) CONFIRM MLIST
grails -- pdf_plugin	XML External Entity (XXE) vulnerability in Grails PDF Plugin 0.6 allows remote attackers to read arbitrary files via a crafted XML document.	2017-02-27	4.3	CVE-2017-6344 BID (link is external) MISC (link is external)
graphicsmagick -- graphicsmagick	The DrawDashPolygon function in magick/render.c in GraphicsMagick before 1.3.24 and the SVG renderer in ImageMagick allow remote attackers to	2017-02-27	4.3	CVE-2016-5240 CONFIRM CONFIRM

	cause a denial of service (infinite loop) by converting a circularly defined SVG file.			MLIST (link is external) MLIST (link is external) MLIST (link is external) BID (link is external)
hashover_project -- hashover	An issue was discovered in HashOver 2.0. The vulnerability exists due to insufficient filtration of user-supplied data passed to the 'hashover/scripts/widget-output.php' URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-02	4.3	CVE-2017-6395 CONFIRM (link is external)
hesiod_project -- hesiod	The hesiod_init function in lib/hesiod.c in Hesiod 3.2.1 compares EUID with UID to determine whether to use configurations from environment variables, which allows local users to gain privileges via the (1) HESIOD_CONFIG or (2) HES_DOMAIN environment variable and leveraging certain SUID/SGUID binary.	2017-03-01	6.9	CVE-2016-10151 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
ibm -- dashboard_application_services_hub	IBM Jazz for Service Management 1.1.2.1 and 1.1.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM Reference #: 1998714.	2017-02-24	6.8	CVE-2016-9975 CONFIRM (link is external) BID (link is external)
ibm -- kenexa_lcms_premier	IBM Kenexa LCMS Premier on Cloud 9.0, and 10.0.0 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM Reference #: 1992067.	2017-03-01	6.5	CVE-2016-9992 CONFIRM (link is external)
ibm -- kenexa_lcms_premier	IBM Kenexa LCMS Premier on Cloud 9.0, and 10.0.0 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM Reference #: 1992067.	2017-03-01	6.5	CVE-2016-9993 CONFIRM (link is external)

ibm -- kenexa_lcms_premier	IBM Kenexa LCMS Premier on Cloud 9.0, and 10.0.0 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM Reference #: 1976805.	2017-03-01	6.5	CVE-2016-9994 CONFIRM (link is external)
ibm -- tivoli_storage_manager	IBM Tivoli Storage Manager Server 7.1 could allow an authenticated user with TSM administrator privileges to cause a buffer overflow using a specially crafted SQL query and execute arbitrary code on the server. IBM Reference #: 1998747.	2017-02-24	6.0	CVE-2016-8998 CONFIRM (link is external) BID (link is external)
ibm -- websphere_mq	IBM WebSphere MQ 8.0 could allow an authenticated user with authority to create a cluster object to cause a denial of service to MQ clustering. IBM Reference #: 1998647.	2017-02-24	4.0	CVE-2016-9009 CONFIRM (link is external) BID (link is external)
iceni -- argus	An exploitable heap corruption vulnerability exists in the loadTrailer functionality of Iceni Argus version 6.6.05. A specially crafted PDF file can cause a heap corruption resulting in arbitrary code execution. An attacker can send/provide a malicious PDF file to trigger this vulnerability.	2017-02-28	6.8	CVE-2016-8715 BID (link is external) MISC (link is external)
imagemagick -- imagemagick	The ReadHDRImage function in coders/hdr.c in ImageMagick 6.x and 7.x allows remote attackers to cause a denial of service (infinite loop) via a crafted HDR file.	2017-02-27	4.3	CVE-2015-8900 CONFIRM CONFIRM CONFIRM MLIST (link is external) MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	ImageMagick 6.x before 6.9.0-5 Beta allows remote attackers to cause a denial of service (infinite loop) via a crafted MIFF file.	2017-02-27	4.3	CVE-2015-8901 CONFIRM CONFIRM MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
imagemagick --	The ReadBlobByte function in coders/pdb.c in	2017-02-27	4.3	CVE-2015-8902

imagemagick	ImageMagick 6.x before 6.9.0-5 Beta allows remote attackers to cause a denial of service (infinite loop) via a crafted PDB file.			CONFIRM CONFIRM MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	The ReadVICARImage function in coders/vicar.c in ImageMagick 6.x before 6.9.0-5 Beta allows remote attackers to cause a denial of service (infinite loop) via a crafted VICAR file.	2017-02-27	4.3	CVE-2015-8903 CONFIRM CONFIRM MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	The ReadGROUP4Image function in coders/tiff.c in ImageMagick before 7.0.1-10 does not check the return value of the fputc function, which allows remote attackers to cause a denial of service (crash) via a crafted image file.	2017-03-03	4.3	CVE-2016-10061 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	The ReadVIFFImage function in coders/viff.c in ImageMagick before 7.0.1-0 allows remote attackers to cause a denial of service (application crash) or other unspecified impact via a crafted file.	2017-03-03	6.8	CVE-2016-10065 SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) MISC (link is external)
imagemagick -- imagemagick	Buffer overflow in the ReadVIFFImage function in coders/viff.c in ImageMagick before 6.9.4-5 allows remote attackers to cause a denial of service (application crash) via a crafted file.	2017-03-03	4.3	CVE-2016-10066 MLIST (link is external) BID (link is external) CONFIRM (link is external)

				CONFIRM (link is external)
imagemagick -- imagemagick	Heap-based buffer overflow in the CalcMinMax function in coders/mat.c in ImageMagick before 6.9.4-0 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted mat file.	2017-03-03	4.3	CVE-2016-10070 SUSE SUSE MLIST (link is external) BID (link is external) MISC (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	coders/tiff.c in ImageMagick before 7.0.3.7 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted image.	2017-03-01	4.3	CVE-2016-9559 MLIST (link is external) MLIST (link is external) BID (link is external) MISC CONFIRM (link is external) CONFIRM (link is external)
intel -- celeron_n2840	Page table walks conducted by the MMU during virtual to physical address translation leave a trace in the last level cache of modern Intel processors. By performing a side-channel attack on the MMU operations, it is possible to leak data and code pointers from JavaScript, breaking ASLR.	2017-02-27	5.0	CVE-2017-5925 MISC (link is external) BID (link is external) MISC (link is external)
intel -- celeron_n2840	Page table walks conducted by the MMU during virtual to physical address translation leave a trace in the last level cache of modern AMD processors. By performing a side-channel attack on the MMU operations, it is possible to leak data and code pointers from JavaScript, breaking ASLR.	2017-02-27	5.0	CVE-2017-5926 MISC (link is external) BID (link is external) MISC (link is external)
intel -- celeron_n2840	Page table walks conducted by the MMU during virtual to physical address translation leave a trace in the last level cache of modern ARM processors. By performing a side-channel attack on the MMU operations, it is possible to leak data and code	2017-02-27	5.0	CVE-2017-5927 MISC (link is external) BID (link is external) MISC (link is

	pointers from JavaScript, breaking ASLR.			external)
intel -- x710_series_driver	Drivers for the Intel Ethernet Controller X710 and Intel Ethernet Controller XL710 families before version 22.0 are vulnerable to a denial of service in certain layer 2 network configurations.	2017-02-27	6.1	CVE-2016-8105 BID (link is external) CONFIRM (link is external)
jasper_project -- jasper	libjasper/include/jasper/jas_math.h in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via vectors involving left shift of a negative value.	2017-03-01	4.3	CVE-2017-5498 BID (link is external) MISC
jasper_project -- jasper	Integer overflow in libjasper/jpc/jpc_dec.c in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-01	4.3	CVE-2017-5499 BID (link is external) MISC
jasper_project -- jasper	libjasper/jpc/jpc_dec.c in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via vectors involving left shift of a negative value.	2017-03-01	4.3	CVE-2017-5500 BID (link is external) MISC
jasper_project -- jasper	Integer overflow in libjasper/jpc/jpc_tsfb.c in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-01	4.3	CVE-2017-5501 BID (link is external) MISC
jasper_project -- jasper	libjasper/jp2/jp2_dec.c in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via vectors involving left shift of a negative value.	2017-03-01	4.3	CVE-2017-5502 BID (link is external) MISC
jasper_project -- jasper	The dec_clnpass function in libjasper/jpc/jpc_t1dec.c in JasPer 1.900.27 allows remote attackers to cause a denial of service (invalid memory write and crash) or possibly have unspecified other impact via a crafted image.	2017-03-01	4.3	CVE-2017-5503 MLIST (link is external) MLIST (link is external) BID (link is external) MISC
jasper_project -- jasper	The jpc_undo_roi function in libjasper/jpc/jpc_dec.c in JasPer 1.900.27 allows remote attackers to cause a denial of service (invalid memory read and crash) via a crafted image.	2017-03-01	4.3	CVE-2017-5504 BID (link is external) MISC
justsystems -- ichitaro	JustSystems Ichitaro 2016 Trial contains a vulnerability that exists when trying to open a specially crafted PowerPoint file. Due to the application incorrectly handling the error case for a function's result, the application will use this result	2017-02-24	6.8	CVE-2017-2791 BID (link is external) MISC (link is external)

	in a pointer calculation for reading file data into. Due to this, the application will read data from the file into an invalid address thus corrupting memory. Under the right conditions, this can lead to code execution under the context of the application.			
kaltura -- kaltura_server	An issue was discovered in Kaltura server Lynx-12.11.0. The vulnerability exists due to insufficient filtration of user-supplied data passed to the "admin_console/web/tools/SimpleJWPlayer.php" URL, the "admin_console/web/tools/AkamaiBroadcaster.php" URL, the "admin_console/web/tools/bigRedButton.php" URL, and the "admin_console/web/tools/bigRedButtonPtsPoc.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-02	4.3	CVE-2017-6391 CONFIRM (link is external) CONFIRM (link is external)
kaltura -- kaltura_server	An issue was discovered in Kaltura server Lynx-12.11.0. The vulnerability exists due to insufficient filtration of user-supplied data passed to the "server-Lynx-12.11.0/admin_console/web/tools/XmlJWPlayer.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-02	4.3	CVE-2017-6392 CONFIRM (link is external) CONFIRM (link is external)
kde -- kdelibs	kpac/script.cpp in KDE kio before 5.32 and kdelibs before 4.14.30 calls the PAC FindProxyForURL function with a full https URL (potentially including Basic Authentication credentials, a query string, or PATH_INFO), which allows remote attackers to obtain sensitive information via a crafted PAC file.	2017-03-02	4.3	CVE-2017-6410 CONFIRM
kodi -- kodi	Directory traversal vulnerability in the Chorus2 2.4.2 add-on for Kodi allows remote attackers to read arbitrary files via a %2E%2E%252e (encoded dot dot slash) in the image path, as demonstrated by image/image%3A%2F%2F%2e%2e%252fetc%252fpasswd.	2017-02-28	5.0	CVE-2017-5982 MISC (link is external) FULLDISC BID (link is external) EXPLOIT-DB (link is external)

lenovo -- xclarity_administrator	Log files generated by Lenovo XClarity Administrator (LXCA) versions earlier than 1.2.2 may contain user credentials in a non-secure, clear text form that could be viewed by a non-privileged user.	2017-03-01	5.0	CVE-2016-8233 BID (link is external) CONFIRM (link is external)
libav -- libav	libavcodec/mpegvideo.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via vectors involving left shift of a negative value.	2017-03-01	4.3	CVE-2016-9819 BID (link is external) MISC
libav -- libav	libavcodec/mpegvideo_motion.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via vectors involving left shift of a negative value.	2017-03-01	4.3	CVE-2016-9820 BID (link is external) MISC
libav -- libav	Integer overflow in libavcodec/mpegvideo_parser.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-01	4.3	CVE-2016-9821 BID (link is external) MISC
libav -- libav	Integer overflow in libavcodec/mpeg12dec.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-01	4.3	CVE-2016-9822 BID (link is external) MISC
libav -- libav	libavcodec/x86/mpegvideo.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-01	4.3	CVE-2016-9823 BID (link is external) MISC
libav -- libav	Integer overflow in libswscale/x86/swscale.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via a crafted file.	2017-03-01	4.3	CVE-2016-9824 BID (link is external) MISC
libav -- libav	libswscale/utils.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via vectors involving left shift of a negative value.	2017-03-01	4.3	CVE-2016-9825 BID (link is external) MISC
libav -- libav	libavcodec/ituh263dec.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via vectors involving left shift of a negative value.	2017-03-01	4.3	CVE-2016-9826 BID (link is external) MISC
libdwarf_project -- libdwarf	dwarf_form.c in libdwarf 20160115 allows remote attackers to cause a denial of service (crash) via a crafted elf file.	2017-02-24	4.3	CVE-2016-5027 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libimobiledevice --	The parse_dict_node function in bplist.c in libplist	2017-03-03	4.3	CVE-2017-5834

libplist	allows attackers to cause a denial of service (out-of-bounds heap read and crash) via a crafted file.			MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libimobiledevice -- libplist	libplist allows attackers to cause a denial of service (large memory allocation and crash) via vectors involving an offset size of zero.	2017-03-03	5.0	CVE-2017-5835 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libimobiledevice -- libplist	The plist_free_data function in plist.c in libplist allows attackers to cause a denial of service (crash) via vectors involving an integer node that is treated as a PLIST_KEY and then triggers an invalid free.	2017-03-03	5.0	CVE-2017-5836 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
libmp3splt_project -- libmp3splt	The splt_cue_export_to_file function in cue.c in libmp3splt 0.9.2 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted file.	2017-03-01	4.3	CVE-2017-5665 BID (link is external) MISC
libtiff -- libtiff	Heap-based buffer overflow in the readContigStripsIntoBuffer function in tif_unix.c in LibTIFF 4.0.7 allows remote attackers to have unspecified impact via a crafted image.	2017-03-01	6.8	CVE-2016-10092 CONFIRM CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external) MISC CONFIRM (link is external)
libtiff -- libtiff	Integer overflow in tools/tiffcp.c in LibTIFF 4.0.7 allows remote attackers to have unspecified impact via a crafted image, which triggers a heap-based buffer overflow.	2017-03-01	6.8	CVE-2016-10093 CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external) MISC CONFIRM (link is external)

libtiff -- libtiff	Off-by-one error in the t2p_readwrite_pdf_image_tile function in tools/tiff2pdf.c in LibTIFF 4.0.7 allows remote attackers to have unspecified impact via a crafted image.	2017-03-01	6.8	CVE-2016-10094 CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external) MISC CONFIRM (link is external)
libtiff -- libtiff	Stack-based buffer overflow in the _TIFFVGetField function in tif_dir.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (crash) via a crafted TIFF file.	2017-03-01	4.3	CVE-2016-10095 CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external) MISC
linux -- linux_kernel	The LLC subsystem in the Linux kernel before 4.9.13 does not ensure that a certain destructor exists in required circumstances, which allows local users to cause a denial of service (BUG_ON) or possibly have unspecified other impact via crafted system calls.	2017-03-01	4.6	CVE-2017-6345 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	Race condition in net/packet/af_packet.c in the Linux kernel before 4.9.13 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a multithreaded application that makes PACKET_FANOUT setsockopt system calls.	2017-03-01	6.9	CVE-2017-6346 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	The hashbin_delete function in net/irda/irqueue.c in the Linux kernel before 4.9.13 improperly manages lock dropping, which allows local users to cause a denial of service (deadlock) via crafted operations on IrDA devices.	2017-03-01	4.9	CVE-2017-6348 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	net/sctp/socket.c in the Linux kernel through 4.10.1	2017-03-01	4.9	CVE-2017-6353

	does not properly restrict association peel-off operations during certain wait states, which allows local users to cause a denial of service (invalid unlock and double free) via a multithreaded application. NOTE: this vulnerability exists because of an incorrect fix for CVE-2017-5986.			CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external)
mp3splt_project -- mp3splt	The free_options function in options_manager.c in mp3splt 2.6.2 allows remote attackers to cause a denial of service (invalid free and crash) via a crafted file.	2017-03-01	4.3	CVE-2017-5666 BID (link is external) MISC
mp3splt_project -- mp3splt	The free_options function in options_manager.c in mp3splt 2.6.2 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted file.	2017-03-01	4.3	CVE-2017-5851 BID (link is external) MISC
nagvis -- nagvis	An issue was discovered in NagVis 1.9b12. The vulnerability exists due to insufficient filtration of user-supplied data passed to the "nagvis-master/share/userfiles/gadgets/std_table.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-02	4.3	CVE-2017-6393 CONFIRM (link is external)
openemr -- openemr	An issue was discovered in OpenEMR 5.0.1-dev. The vulnerability exists due to insufficient filtration of user-supplied data passed to the "openemr-master/gacl/admin/object_search.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-02	4.3	CVE-2017-6394 MISC (link is external)
opensuse_project -- opensuse	The wrap_lines_smart function in ass_render.c in libass before 0.13.4 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors, related to "0/3 line wrapping equalization."	2017-03-03	5.0	CVE-2016-7969 SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) FEDORA FEDORA

				FEDORA GENTOO
opensuse_project -- opensuse	The check_allocations function in libass/ass_shaper.c in libass before 0.13.4 allows remote attackers to cause a denial of service (memory allocation failure) via unspecified vectors.	2017-03-03	5.0	CVE-2016-7972 SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) FEDORA FEDORA FEDORA GENTOO
opensuse_project -- opensuse	The MagickRealloc function in memory.c in Graphicsmagick 1.3.25 allows remote attackers to cause a denial of service (crash) via large dimensions in a jpeg image.	2017-03-01	4.3	CVE-2016-9830 CONFIRM (link is external) SUSE DEBIAN MLIST (link is external) BID (link is external) MISC CONFIRM (link is external)
pingidentity -- mod_auth_openidc	The "OpenID Connect Relying Party and OAuth 2.0 Resource Server" (aka mod_auth_openidc) module before 2.1.5 for the Apache HTTP Server does not skip OIDC_CLAIM_ and OIDCAuthNHeader headers in an "OIDCUnAuthAction pass" configuration, which allows remote attackers to bypass authentication via crafted HTTP traffic.	2017-03-02	5.0	CVE-2017-6062 CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
pingidentity -- mod_auth_openidc	The "OpenID Connect Relying Party and OAuth 2.0 Resource Server" (aka mod_auth_openidc) module before 2.1.6 for the Apache HTTP Server does not skip OIDC_CLAIM_ and OIDCAuthNHeader headers in an "AuthType oauth20" configuration, which allows remote attackers to bypass authentication via crafted HTTP traffic.	2017-03-02	5.0	CVE-2017-6413 CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
plone -- plone	Plone 3.3 through 5.1a1 allows remote attackers to	2017-02-24	5.0	CVE-2016-4042 MLIST (link is

	obtain information about the ID of sensitive content via unspecified vectors.			external) CONFIRM
podofo_project -- podofo	The PoDoFo::PdfPage::GetInheritedKeyFromObject function in base/PdfVariant.cpp in PoDoFo 0.9.4 allows remote attackers to cause a denial of service (infinite loop) via a crafted file.	2017-03-01	4.3	CVE-2017-5852 MLIST (link is external) MLIST (link is external) MISC
podofo_project -- podofo	Integer overflow in base/PdfParser.cpp in PoDoFo 0.9.4 allows remote attackers to have unspecified impact via a crafted file.	2017-03-01	6.8	CVE-2017-5853 BID (link is external) MISC
podofo_project -- podofo	base/PdfOutputStream.cpp in PoDoFo 0.9.4 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted file.	2017-03-01	4.3	CVE-2017-5854 MLIST (link is external) MLIST (link is external) BID (link is external) MISC
podofo_project -- podofo	The PoDoFo::PdfParser::ReadXRefSubsection function in PdfParser.cpp in PoDoFo 0.9.4 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.	2017-03-01	4.3	CVE-2017-5855 BID (link is external) MISC
podofo_project -- podofo	Heap-based buffer overflow in the PoDoFo::PdfTokenizer::GetNextToken function in PdfTokenizer.cpp in PoDoFo 0.9.4 allows remote attackers to have unspecified impact via a crafted file.	2017-03-01	6.8	CVE-2017-5886 BID (link is external) MISC
radare -- radare2	The dex_parse_debug_item function in libr/bin/p/bin_dex.c in radare2 1.2.1 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted DEX file.	2017-03-01	6.8	CVE-2017-6319 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
radare -- radare2	The dex_loadcode function in libr/bin/p/bin_dex.c in radare2 1.2.1 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted DEX file.	2017-03-01	4.3	CVE-2017-6387 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
radare -- radare2	The dex_parse_debug_item function in libr/bin/p/bin_dex.c in radare2 1.2.1 allows remote	2017-03-01	4.3	CVE-2017-6415 BID (link is

	attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DEX file.			external) CONFIRM (link is external) CONFIRM (link is external)
revive-adserver -- revive_adserver	Session fixation vulnerability in the forgot password mechanism in Revive Adserver before 4.0.1, when setting a new password, allows remote attackers to hijack web sessions via the session ID.	2017-03-03	5.5	CVE-2017-5831 MLIST (link is external) CONFIRM (link is external)
revive-adserver -- revive_adserver	Cross-site scripting (XSS) vulnerability in the invocation code generation for interstitial zones in Revive Adserver before 4.0.1 allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.	2017-03-03	4.3	CVE-2017-5833 MLIST (link is external) CONFIRM (link is external)
siemens -- ruggedcom_network_management_software	A non-privileged user of the Siemens web application RUGGEDCOM NMS < V1.2 on port 8080/TCP and 8081/TCP could perform a persistent Cross-Site Scripting (XSS) attack, potentially resulting in obtaining administrative permissions.	2017-02-27	4.3	CVE-2017-2683 BID (link is external) CONFIRM (link is external)
soruly -- whatanime.ga	An issue was discovered in whatanime.ga before c334dd8499a681587dd4199e90b0aa0eba814c1d. The vulnerability exists due to insufficient filtration of user-supplied data passed to the "whatanime.ga-master/index.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-02	4.3	CVE-2017-6390 CONFIRM (link is external) CONFIRM (link is external)
tigervnc -- tigervnc	The Xvnc server in TigerVNC allows remote attackers to cause a denial of service (invalid memory access and crash) by terminating a TLS handshake early.	2017-02-28	5.0	CVE-2016-10207 SUSE MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
tigervnc -- tigervnc	Buffer overflow in the ModifiablePixelBuffer::fillRect function in TigerVNC before 1.7.1 allows remote servers to execute arbitrary code via an RRE	2017-02-28	6.8	CVE-2017-5581 MLIST (link is external) MLIST (link is

	message with subrectangle outside framebuffer boundaries.			external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
veritas -- netbackup_appliance	An issue was discovered in Veritas NetBackup before 8.0 and NetBackup Appliance before 3.0. Local arbitrary command execution can occur when using bpcd and bpnbat.	2017-03-02	4.6	CVE-2017-6401 CONFIRM (link is external)
veritas -- netbackup_appliance	An issue was discovered in Veritas NetBackup 8.0 and earlier and NetBackup Appliance 3.0 and earlier. Denial of service affecting NetBackup server can occur.	2017-03-02	4.0	CVE-2017-6402 CONFIRM (link is external)
veritas -- netbackup_appliance	An issue was discovered in Veritas NetBackup 8.0 and earlier and NetBackup Appliance 3.0 and earlier. Hostname-based security is open to DNS spoofing.	2017-03-02	5.0	CVE-2017-6405 CONFIRM (link is external)
veritas -- netbackup_appliance	An issue was discovered in Veritas NetBackup 8.0 and earlier and NetBackup Appliance 3.0 and earlier. A local-privilege-escalation race condition in pbx_exchange can occur when a local user connects to a socket before permissions are secured.	2017-03-02	4.4	CVE-2017-6408 CONFIRM (link is external)
webpagetest_project -- webpagetest	An issue was discovered in WPO-Foundation WebPageTest 3.0. The vulnerability exists due to insufficient filtration of user-supplied data passed to the "webpagetest-master/www/compare-cf.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-02	4.3	CVE-2017-6396 CONFIRM (link is external)
xen -- xen	Xen through 4.7.x allows local ARM guest OS users to cause a denial of service (host panic) by sending an asynchronous abort.	2017-02-27	4.9	CVE-2016-9815 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM

				CONFIRM
xen -- xen	Xen through 4.7.x allows local ARM guest OS users to cause a denial of service (host crash) via vectors involving an asynchronous abort while at EL2.	2017-02-27	4.9	CVE-2016-9816 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM
xen -- xen	Xen through 4.7.x allows local ARM guest OS users to cause a denial of service (host crash) via vectors involving a (1) data or (2) prefetch abort with the ESR_EL2.EA bit set.	2017-02-27	4.9	CVE-2016-9817 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM CONFIRM
xen -- xen	Xen through 4.7.x allows local ARM guest OS users to cause a denial of service (host crash) via vectors involving an asynchronous abort while at HYP.	2017-02-27	4.9	CVE-2016-9818 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM
yandex -- yandex_browser	Yandex Browser for iOS before 16.10.0.2357 does not properly restrict processing of facetime:// URLs, which allows remote attackers to initiate facetime-call without user's approval and obtain video and audio data from a device via a crafted web site.	2017-03-01	4.3	CVE-2016-8507 BID (link is external) CONFIRM (link is external)
yandex -- yandex_browser	Yandex Browser for desktop before 17.1.1.227 does not show Protect (similar to Safebrowsing in Chromium) warnings in web-sites with special content-type, which could be used by remote attacker for prevention Protect warning on own malicious web-site.	2017-03-01	4.3	CVE-2016-8508 BID (link is external) CONFIRM (link is external)
ysurac -- flightairmap	An issue was discovered in FlightAirMap v1.0-beta.10. The vulnerability exists due to insufficient filtration of user-supplied data in multiple parameters passed to several *-sub-menu.php pages. An attacker could execute arbitrary HTML	2017-03-02	4.3	CVE-2017-6397 CONFIRM (link is external)

	and script code in a browser in the context of the vulnerable website.			
zziplib_project -- zziplib	Heap-based buffer overflow in the __zzip_get32 function in fetch.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (crash) via a crafted ZIP file.	2017-03-01	4.3	CVE-2017-5974 MLIST (link is external) MISC
zziplib_project -- zziplib	Heap-based buffer overflow in the __zzip_get64 function in fetch.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (crash) via a crafted ZIP file.	2017-03-01	4.3	CVE-2017-5975 MLIST (link is external) MISC
zziplib_project -- zziplib	Heap-based buffer overflow in the zzip_mem_entry_extra_block function in memdisk.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (crash) via a crafted ZIP file.	2017-03-01	4.3	CVE-2017-5976 MLIST (link is external) MISC
zziplib_project -- zziplib	The zzip_mem_entry_extra_block function in memdisk.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (invalid memory read and crash) via a crafted ZIP file.	2017-03-01	4.3	CVE-2017-5977 MLIST (link is external) MISC
zziplib_project -- zziplib	The zzip_mem_entry_new function in memdisk.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted ZIP file.	2017-03-01	4.3	CVE-2017-5978 MISC
zziplib_project -- zziplib	The prescan_entry function in fseeko.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted ZIP file.	2017-03-01	4.3	CVE-2017-5979 MISC
zziplib_project -- zziplib	The zzip_mem_entry_new function in memdisk.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted ZIP file.	2017-03-01	4.3	CVE-2017-5980 MISC
zziplib_project -- zziplib	seeko.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (assertion failure and crash) via a crafted ZIP file.	2017-03-01	4.3	CVE-2017-5981 MISC

Low Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
dropbear_ssh_project -- dropbear_ssh	The dbclient and server in Dropbear SSH before 2016.74, when compiled with DEBUG_TRACE, allows local users to read process memory via the -v argument, related to a failed remote ident.	2017-03-03	2.1	CVE-2016-7409 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) GENTOO
ibm -- connections	IBM Connections 4.0, 4.5, 5.0, and 5.5 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 #: 1998294.	2017-03-01	3.5	CVE-2016-5932 CONFIRM (link is external) BID (link is external)
ibm -- qradar_security_information_and_event_manager	IBM QRadar 7.2 uses outdated hashing algorithms to hash certain passwords, which could allow a local user to obtain and decrypt user credentials. IBM Reference #: 1997341.	2017-03-01	2.1	CVE-2016-2879 CONFIRM (link is external) BID (link is external)
ibm -- qradar_security_information_and_event_manager	IBM QRadar 7.2 stores the encryption key used to encrypt the service account password which can be obtained by a local user. IBM Reference #: 1997340.	2017-03-01	2.1	CVE-2016-2880 CONFIRM (link is external)
plone -- plone	Chameleon (five.pt) in Plone 5.0rc1 through 5.1a1 allows remote authenticated users to bypass Restricted Python by leveraging permissions to create or edit templates.	2017-02-24	3.5	CVE-2016-4043 MLIST (link is external) CONFIRM
qemu -- qemu	The virgl_cmd_get_capset function in hw/display/virtio-gpu-3d.c in QEMU (aka Quick Emulator) built with Virtio GPU Device emulator support allows local guest OS users to cause a denial of service (out-of-bounds read and process crash) via	2017-02-27	2.1	CVE-2016-10028 CONFIRM MLIST (link is external) MLIST (link is

	a VIRTIO_GPU_CMD_GET_CAPSET command with a maximum capabilities size with a value of 0.			external) BID (link is external) SECTRACK (link is external) MLIST
qemu -- qemu	The virtio_gpu_set_scanout function in QEMU (aka Quick Emulator) built with Virtio GPU Device emulator support allows local guest OS users to cause a denial of service (out-of-bounds read and process crash) via a scanout id in a VIRTIO_GPU_CMD_SET_SCANOUT command larger than num_scanouts.	2017-02-27	2.1	CVE-2016-10029 CONFIRM CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external) SECTRACK (link is external)
revive-adserver -- revive_adserver	Cross-site scripting (XSS) vulnerability in Revive Adserver before 4.0.1 allows remote authenticated users to inject arbitrary web script or HTML via the user's email address.	2017-03-03	3.5	CVE-2017-5832 MLIST (link is external) CONFIRM (link is external)
tenable -- log_correlation_engine	Cross-site scripting (XSS) vulnerability in Tenable Log Correlation Engine (aka LCE) before 4.8.1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	2017-02-28	3.5	CVE-2016-9261 CONFIRM (link is external)
tenable -- nessus	Cross-site scripting (XSS) vulnerability in Tenable Nessus before 6.9.1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	2017-02-28	3.5	CVE-2016-9259 SECTRACK (link is external) CONFIRM (link is external)
veritas -- netbackup_appliance	An issue was discovered in Veritas NetBackup Before 7.7 and NetBackup Appliance Before 2.7. There are world-writable log files, allowing destruction or spoofing of log data.	2017-03-02	2.1	CVE-2017-6404 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).