Vulnerability Summary for the Week of March 13 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**
adobe -- flash_player	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable buffer overflow / underflow vulnerability in the Primetime TVSDK that supports customizing ad information. Successful exploitation could lead to arbitrary code execution.	2017-03-14	10.0	CVE-2017-2997 BID (link is external) CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable memory corruption vulnerability in the Primetime TVSDK API functionality related to timeline interactions. Successful exploitation could lead to arbitrary code execution.	2017-03-14	10.0	CVE-2017-2998 BID (link is external) CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable memory corruption vulnerability in the Primetime TVSDK functionality related to hosting playback surface. Successful exploitation could lead to arbitrary code execution.	2017-03-14	10.0	CVE-2017-2999 BID (link is external) CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.221 and	2017-03-14	10.0	CVE-2017-3001 BID (link is

	earlier have an exploitable use after free vulnerability related to garbage collection in the ActionScript 2 VM. Successful exploitation could lead to arbitrary code execution.			external) CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability in the ActionScript2 TextField object related to the variable property. Successful exploitation could lead to arbitrary code execution.	2017-03-14	10.0	CVE-2017-3002 BID (link is external) CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability related to an interaction between the privacy user interface and the ActionScript 2 Camera object. Successful exploitation could lead to arbitrary code execution.	2017-03-14	10.0	CVE-2017-3003 BID (link is external) CONFIRM (link is external)
alienvault -- ossim	The logcheck function in session.inc in AlienVault OSSIM before 5.3.1, when an action has been created, and USM before 5.3.1 allows remote attackers to bypass authentication and consequently obtain sensitive information, modify the application, or execute arbitrary code as root via an "AV Report Scheduler" HTTP User-Agent header.	2017-03-15	7.5	CVE-2016-7955 BUGTRAQ (link is external) MISC (link is external) CONFIRM (link is external)
apache -- struts	The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 mishandles file upload, which allows remote attackers to execute arbitrary commands via a #cmd= string in a crafted Content-Type HTTP header, as exploited in the wild in March 2017.	2017-03-10	10.0	CVE-2017-5638 MISC (link is external) MISC (link is external) MISC (link is external) BID (link is external) MISC (link is external) CONFIRM EXPLOIT-DB (link is external) CONFIRM CONFIRM MISC (link is external) MISC (link is

				external) MISC (link is external) MISC MISC (link is external) MISC (link is external)
azure_dex -- data_expert_ultimate	In Azure Data Expert Ultimate 2.2.16, the SMTP verification function suffers from a buffer overflow vulnerability, leading to remote code execution. The attack vector is a crafted SMTP daemon that sends a long 220 (aka "Service ready") string.	2017-03-10	7.5	CVE-2017-6506 MISC (link is external) BID (link is external) EXPLOIT-DB (link is external)
bitlbee -- bitlbee	Use-after-free vulnerability in bitlbee-libpurple before 3.5 allows remote servers to cause a denial of service (crash) or possibly execute arbitrary code by causing a file transfer connection to expire.	2017-03-14	7.5	CVE-2016-10188 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM
bitlbee -- bitlbee-libpurple	bitlbee-libpurple before 3.5.1 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) and possibly execute arbitrary code via a file transfer request for a contact that is not in the contact list. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-10189.	2017-03-14	7.5	CVE-2017-5668 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM (link is external)
cambium_networks -- cnpilot_r200_series_firmware	On Cambium Networks cnPilot R200/201 devices before 4.3, there is a vulnerability involving the certificate of the device and its RSA keys, aka RBN-183.	2017-03-10	10.0	CVE-2017-5859 CONFIRM (link is external)
embedthis -- goahead	A command-injection vulnerability exists in a web application on a custom-built GoAhead web server used on Foscam, Vstarcam, and multiple white-label IP camera models. The mail-sending form in the mail.htm page allows an attacker to inject a command into the receiver1 field in the form; it will be executed with root privileges.	2017-03-13	9.0	CVE-2017-5675 MISC (link is external) MISC (link is external)

f-secure -- software_updater	F-Secure Software Updater 2.20, as distributed in several F-Secure products, downloads installation packages over plain http and does not perform file integrity validation after download. Man-in-the-middle attackers can replace the file with their own executable which will be executed under the SYSTEM account. Note that when Software Updater is configured to install updates automatically, it checks if the downloaded file is digitally signed by default, but does not check the author of the signature. When running in manual mode (default), no signature check is performed.	2017-03-11	9.3	CVE-2017-6466 MISC BID (link is external)
imagemagick -- imagemagick	Memory leak in the IsOptionMember function in MagickCore/option.c in ImageMagick before 6.9.2-2, as used in ODR-PadEnc and other products, allows attackers to trigger memory consumption.	2017-03-14	7.8	CVE-2016-10252 CONFIRM CONFIRM CONFIRM (link is external)
imagemagick -- imagemagick	The gnuplot delegate functionality in ImageMagick before 6.9.4-0 and GraphicsMagick allows remote attackers to execute arbitrary commands via unspecified vectors.	2017-03-15	7.5	CVE-2016-5239 MISC MLIST (link is external) BID (link is external)
libgd -- libgd	Integer underflow in the _gdContributionsAlloc function in gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to have unspecified impact via vectors related to decrementing the u variable.	2017-03-15	7.5	CVE-2016-10166 CONFIRM (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
logback -- logback	QOS.ch Logback before 1.2.0 has a serialization vulnerability affecting the SocketServer and ServerSocketReceiver components.	2017-03-13	7.5	CVE-2017-5929 CONFIRM (link is external)
microsoft -- edge	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory. The vulnerability could	2017-03-16	7.6	CVE-2017-0034 BID (link is external) CONFIRM (link is external)

	corrupt memory in a way that enables an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.			
microsoft -- internet_explorer	The scripting engine in Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." This vulnerability is different from that described in CVE-2017-0130.	2017-03-16	7.6	CVE-2017-0040 BID (link is external) CONFIRM (link is external)
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability." This vulnerability is different from those described in CVE-2017-0018 and CVE-2017-0037.	2017-03-16	7.6	CVE-2017-0149 BID (link is external) CONFIRM (link is external)
microsoft -- server_message_block	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.	2017-03-16	9.3	CVE-2017-0143 BID (link is external) CONFIRM (link is external)
microsoft -- server_message_block	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and	2017-03-16	9.3	CVE-2017-0144 BID (link is external) CONFIRM (link is external)

	Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.			
microsoft -- server_message_block	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0146, and CVE-2017-0148.	2017-03-16	9.3	CVE-2017-0145 BID (link is external) CONFIRM (link is external)
microsoft -- server_message_block	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, and CVE-2017-0148.	2017-03-16	9.3	CVE-2017-0146 BID (link is external) CONFIRM (link is external)
microsoft -- server_message_block	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0145,	2017-03-16	9.3	CVE-2017-0148 BID (link is external) CONFIRM (link is external)

	and CVE-2017-0146.			
microsoft -- windows_10	The PDF library in Microsoft Edge; Windows 8.1; Windows Server 2012 and R2; Windows RT 8.1; and Windows 10, 1511, and 1607 allows remote attackers to execute arbitrary code via a crafted PDF file, aka "Microsoft PDF Remote Code Execution Vulnerability."	2017-03-16	7.6	CVE-2017-0023 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka "Uniscribe Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090.	2017-03-16	9.3	CVE-2017-0083 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka "Uniscribe Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090.	2017-03-16	9.3	CVE-2017-0086 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka "Uniscribe Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090.	2017-03-16	9.3	CVE-2017-0087 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka	2017-03-16	9.3	CVE-2017-0088 BID (link is external) CONFIRM (link is external)

	"Windows Uniscribe Remote Code Execution Vulnerability."			
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka "Uniscribe Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, and CVE-2017-0090.	2017-03-16	9.3	CVE-2017-0089 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka "Uniscribe Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, and CVE-2017-0089.	2017-03-16	9.3	CVE-2017-0090 BID (link is external) CONFIRM (link is external)
mikrotik -- router_hap_lite_firmware	The MikroTik Router hAP Lite 6.25 has no protection mechanism for unsolicited TCP ACK packets in the case of a fast network connection, which allows remote attackers to cause a denial of service (CPU consumption) by sending many ACK packets. After the attacker stops the exploit, the CPU usage is 100% and the router requires a reboot for normal operation.	2017-03-12	7.8	CVE-2017-6444 MISC (link is external) MISC (link is external) MISC (link is external)
novell -- iprint	Remote attackers can use the iPrint web-browser ActiveX plugin in Novell iPrint Client before 5.42 for Windows XP/Vista/Win7 to execute code by overflowing the "name" parameter.	2017-03-11	9.3	CVE-2010-4314 CONFIRM (link is external)
oneplus -- oxygenos	An issue was discovered in OxygenOS before 4.0.3 for OnePlus 3 and 3T. The attacker can persistently make the (locked) bootloader start the platform with dm-verity disabled, by issuing the 'fastboot oem disable_dm_verity' command. Having dm-verity disabled, the kernel will not	2017-03-12	10.0	CVE-2017-5624 MISC (link is external)

	verify the system partition (and any other dm-verity protected partition), which may allow for persistent code execution and privilege escalation.			
oneplus -- oxygenos	OxygenOS before version 4.0.2, on OnePlus 3 and 3T, has two hidden fastboot oem commands (4F500301 and 4F500302) that allow the attacker to lock/unlock the bootloader, disregarding the 'OEM Unlocking' checkbox, without user confirmation and without a factory reset. This allows for persistent code execution with high privileges (kernel/root) with complete access to user data.	2017-03-12	10.0	CVE-2017-5626 MISC (link is external)
pharos -- popup	An exploitable buffer overflow exists in the psnotifyd application of the Pharos PopUp printer client version 9.0. A specially crafted packet can be sent to the victim's computer and can lead to a heap based buffer overflow resulting in remote code execution. This client is always listening, has root privileges, and requires no user interaction to exploit.	2017-03-10	10.0	CVE-2017-2785 BID (link is external) MISC (link is external)
pharos -- popup	A buffer overflows exists in the psnotifyd application of the Pharos PopUp printer client version 9.0. A specially crafted packet can be sent to the victim's computer and can lead to a heap based buffer overflow resulting in potential remote code execution. This client is always listening, has root privileges, and requires no user interaction to exploit.	2017-03-10	9.3	CVE-2017-2787 BID (link is external) MISC (link is external)
pharos -- popup	A buffer overflows exists in the psnotifyd application of the Pharos PopUp printer client version 9.0. A specially crafted packet can be sent to the victim's computer and can lead to a heap based buffer overflow resulting in potential remote code execution. This client is always listening, has root privileges, and requires no user interaction to exploit.	2017-03-10	10.0	CVE-2017-2788 BID (link is external) MISC (link is external)
trend_micro --	Trend Micro Endpoint Sensor 1.6 before b1290	2017-03-10	9.3	CVE-2017-6798 BID (link is

endpoint_sensor	has a DLL hijacking vulnerability that allows remote attackers to execute arbitrary code, aka Trend Micro Vulnerability Identifier 2015-0208.			external) CONFIRM (link is external)
trendmicro -- interscan_messaging_security_virtual_appliance	An issue was discovered in Trend Micro InterScan Messaging Security (Virtual Appliance) 9.1-1600. An authenticated user can execute a terminal command in the context of the web server user (which is root). Besides, the default installation of IMSVA comes with default administrator credentials. The saveCert.imss endpoint takes several user inputs and performs blacklisting. After that, it uses them as arguments to a predefined operating-system command without proper sanitization. However, because of an improper blacklisting rule, it's possible to inject arbitrary commands into it.	2017-03-14	9.0	CVE-2017-6398 BID (link is external) MISC (link is external)
trendnet -- tew-812dru_firmware	Buffer overflow in Broadcom ACSD allows remote attackers to execute arbitrary code via a long string to TCP port 5916. This component is used on routers of multiple vendors including ASUS RT-AC66U and TRENDnet TEW-812DRU.	2017-03-14	10.0	CVE-2013-4659 MISC (link is external) MISC (link is external)
umn -- mapserver	Stack-based buffer overflow in MapServer before 6.0.6, 6.2.x before 6.2.4, 6.4.x before 6.4.5, and 7.0.x before 7.0.4 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via vectors involving WFS get feature requests.	2017-03-15	7.5	CVE-2017-5522 DEBIAN CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM (link is external) MLIST
zammad -- zammad	An issue was discovered in Zammad before 1.0.4, 1.1.x before 1.1.3, and 1.2.x before 1.2.1. Attackers can login with the hashed password itself (e.g., from the DB) instead of the valid password string.	2017-03-13	7.5	CVE-2017-5619 BID (link is external) CONFIRM (link is external)
zammad -- zammad	An issue was discovered in Zammad before 1.0.4, 1.1.x before 1.1.3, and 1.2.x before 1.2.1, caused by lack of a protection mechanism involving HTTP Access-Control headers. To exploit the vulnerability, an attacker can send cross-domain	2017-03-13	7.5	CVE-2017-6080 BID (link is external) CONFIRM (link is external)

	requests directly to the REST API for users with a valid session cookie and receive the result.			

Medium Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
adobe -- flash_player	Adobe Flash Player versions 24.0.0.221 and earlier have a vulnerability in the random number generator used for constant blinding. Successful exploitation could lead to information disclosure.	2017-03-14	5.0	CVE-2017-3000 BID (link is external) CONFIRM (link is external)
adobe -- shockwave_player	Adobe Shockwave versions 12.2.7.197 and earlier have an insecure library loading (DLL hijacking) vulnerability. Successful exploitation could lead to escalation of privilege.	2017-03-14	6.8	CVE-2017-2983 BID (link is external) CONFIRM (link is external)
apache -- tomcat	An information disclosure issue was discovered in Apache Tomcat 8.5.7 to 8.5.9 and 9.0.0.M11 to 9.0.0.M15 in reverse-proxy configurations. Http11InputBuffer.java allows remote attackers to read data that was intended to be associated with a different request.	2017-03-14	5.0	CVE-2016-8747 CONFIRM CONFIRM CONFIRM CONFIRM BID (link is external)
appneta -- tcpreplay	Buffer overflow in the tcpcapinfo utility in Tcpreplay before 4.2.0 Beta 1 allows remote attackers to have unspecified impact via a pcap file with an over-size packet.	2017-03-15	6.8	CVE-2017-6429 BUGTRAQ (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
artifex -- mupdf	Buffer overflow in the main function in jstest_main.c in Mujstest in Artifex Software, Inc.	2017-03-16	4.3	CVE-2016-10246 CONFIRM (link

	MuPDF before 1.10 allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted file.			is external) MLIST (link is external) MISC
artifex -- mupdf	Buffer overflow in the my_getline function in jstest_main.c in Mujstest in Artifex Software, Inc. MuPDF before 1.10 allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted file.	2017-03-16	4.3	CVE-2016-10247 CONFIRM (link is external) MLIST (link is external) MISC
artifex -- mupdf	Stack-based buffer overflow in jstest_main.c in mujstest in Artifex Software, Inc. MuPDF 1.10a allows remote attackers to have unspecified impact via a crafted image.	2017-03-15	6.8	CVE-2017-6060 MLIST (link is external) MISC MISC (link is external)
audiofile -- audiofile	Heap-based buffer overflow in the MSADPCM::initializeCoefficients function in MSADPCM.cpp in audiofile (aka libaudiofile and Audio File Library) 0.3.6 allows remote attackers to have unspecified impact via a crafted audio file.	2017-03-15	6.8	CVE-2017-6827 MISC
audiofile -- audiofile	Heap-based buffer overflow in the readValue function in FileHandle.cpp in audiofile (aka libaudiofile and Audio File Library) 0.3.6 allows remote attackers to have unspecified impact via a crafted WAV file.	2017-03-15	6.8	CVE-2017-6828 MISC
bigtreecms -- bigtree_cms	CSRF exists in BigTree CMS 4.1.18 and 4.2.16 with the id parameter to the admin/ajax/users/delete/ page. A user can be deleted.	2017-03-15	5.8	CVE-2017-6914 MISC (link is external) MISC (link is external)
bigtreecms -- bigtree_cms	CSRF exists in BigTree CMS 4.1.18 with the colophon parameter to the admin/settings/update/ page. The Colophon can be changed.	2017-03-15	4.3	CVE-2017-6915 MISC (link is external) MISC (link is external)
bigtreecms -- bigtree_cms	CSRF exists in BigTree CMS 4.1.18 with the nav-social[#] parameter to the admin/settings/update/ page. The Navigation Social can be changed.	2017-03-15	4.3	CVE-2017-6916 MISC (link is external) MISC (link is external)
bigtreecms -- bigtree_cms	CSRF exists in BigTree CMS 4.2.16 with the value parameter to the admin/settings/update/ page. The Colophon can be changed.	2017-03-15	4.3	CVE-2017-6917 MISC (link is external) MISC (link is

				external)
bigtreecms -- bigtree_cms	CSRF exists in BigTree CMS 4.2.16 with the value[#][*] parameter to the admin/settings/update/ page. The Navigation Social can be changed.	2017-03-15	4.3	CVE-2017-6918 MISC (link is external) MISC (link is external)
bitlbee -- bitlbee-libpurple	BitlBee before 3.5 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) and possibly execute arbitrary code via a file transfer request for a contact that is not in the contact list.	2017-03-14	5.0	CVE-2016-10189 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM (link is external)
cerberusftp -- ftp_server	In Cerberus FTP Server 8.0.10.1, a crafted HTTP request causes the Windows service to crash. The attack methodology involves a long Host header and an invalid Content-Length header.	2017-03-14	5.0	CVE-2017-6367 BID (link is external) EXPLOIT-DB (link is external)
debian -- debian_linux	Stack-based buffer overflow in the evutil_parse_sockaddr_port function in evutil.c in libevent before 2.1.6-beta allows attackers to cause a denial of service (segmentation fault) via vectors involving a long string in brackets in the ip_as_string argument.	2017-03-15	5.0	CVE-2016-10196 DEBIAN MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
debian -- debian_linux	The search_make_new function in evdns.c in libevent before 2.1.6-beta allows attackers to cause a denial of service (out-of-bounds read) via an empty hostname.	2017-03-15	5.0	CVE-2016-10197 DEBIAN MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)

				CONFIRM (link is external)
digisol -- dg-hr1400_router_firmware	Privilege escalation vulnerability on the DIGISOL DG-HR1400 1.00.02 wireless router enables an attacker to escalate from user privilege to admin privilege just by modifying the Base64-encoded session cookie value.	2017-03-14	6.5	CVE-2017-6896 MISC (link is external) MISC (link is external)
drupal -- drupal	Some administrative paths in Drupal 8.2.x before 8.2.7 did not include protection for CSRF. This would allow an attacker to disable some blocks on a site. This issue is mitigated by the fact that users would have to know the block ID.	2017-03-16	5.1	CVE-2017-6379 BID (link is external) CONFIRM
eaton -- xcomfort_ethernet_communication_interface	An issue was discovered in Eaton xComfort Ethernet Communication Interface (ECI) Versions 1.07 and prior. By accessing a specific uniform resource locator (URL) on the webserver, a malicious user may be able to access files without authenticating.	2017-03-14	5.0	CVE-2016-9368 MISC
embedthis -- goahead	A vulnerability in a custom-built GoAhead web server used on Foscam, Vstarcam, and multiple white-label IP camera models allows an attacker to craft a malformed HTTP ("GET system.ini HTTP/1.1\n\n" - note the lack of "/" in the path field of the request) request that will disclose the configuration file with the login password.	2017-03-13	5.0	CVE-2017-5674 MISC (link is external) MISC (link is external)
epson -- tmnet_webconfig	Cross-site scripting (XSS) vulnerability in EPSON TMNet WebConfig 1.00 allows remote attackers to inject arbitrary web script or HTML via the W_AD1 parameter to Forms/oadmin_1.	2017-03-15	4.3	CVE-2017-6443 FULLDISC BID (link is external) EXPLOIT-DB (link is external)
ettercap -- ettercap	The compile_tree function in ef_compiler.c in the Etterfilter utility in Ettercap 0.8.2 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted filter.	2017-03-15	4.3	CVE-2017-6430 BUGTRAQ (link is external) BID (link is external) MISC (link is external) MISC (link is external)
evostream -- media_server	A Buffer Overflow was discovered in EvoStream Media Server 1.7.1. A crafted HTTP request with a malicious header will cause a crash. An example	2017-03-10	5.0	CVE-2017-6427 BID (link is external) EXPLOIT-DB

	attack methodology may include a long message-body in a GET request.			(link is external)
fiyo -- fiyo_cms	Fiyo CMS 2.0.6.1 allows remote authenticated users to gain privileges via a modified level parameter to dapur/ in an app=user&act=edit action.	2017-03-12	6.5	CVE-2017-6823 MISC (link is external) BID (link is external)
gnu -- glibc	Integer overflow in the strxfrm function in the GNU C Library (aka glibc or libc6) before 2.21 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a stack-based buffer overflow.	2017-03-15	6.8	CVE-2015-8982 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM CONFIRM
graphicsmagick -- graphicsmagick	The QuantumTransferMode function in coders/tiff.c in GraphicsMagick 1.3.25 and earlier allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a small samples per pixel value in a CMYKA TIFF file.	2017-03-14	4.3	CVE-2017-6335 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
hikvision -- ds-76xxx_series_firmware	Buffer overflow on Hikvision NVR DS-76xxNI-E1/2 and DS-77xxxNI-E4 devices before 3.4.0 allows remote authenticated users to cause a denial of service (service interruption) via a crafted HTTP request, aka the PSIA issue.	2017-03-13	6.8	CVE-2015-4407 CONFIRM (link is external)
hikvision -- ds-76xxx_series_firmware	Buffer overflow on Hikvision NVR DS-76xxNI-E1/2 and DS-77xxxNI-E4 devices before 3.4.0 allows remote authenticated users to cause a denial of service (service interruption) via a crafted HTTP request, aka the ISAPI issue.	2017-03-13	6.8	CVE-2015-4408 CONFIRM (link is external)
hikvision -- ds-76xxx_series_firmware	Buffer overflow on Hikvision NVR DS-76xxNI-E1/2 and DS-77xxxNI-E4 devices before 3.4.0 allows remote authenticated users to cause a denial of service (service interruption) via a crafted HTTP request, aka the SDK issue.	2017-03-13	6.8	CVE-2015-4409 CONFIRM (link is external)
imagemagick -- imagemagick	Double free vulnerability in coders/tga.c in ImageMagick 7.0.0 and later allows remote attackers to cause a denial of service (application	2017-03-15	4.3	CVE-2015-8894 MLIST (link is external) MISC (link is

	crash) via a crafted tga file.			external) CONFIRM (link is external)
imagemagick -- imagemagick	Integer overflow in coders/icon.c in ImageMagick 6.9.1-3 and later allows remote attackers to cause a denial of service (application crash) via a crafted length value, which triggers a buffer overflow.	2017-03-15	5.0	CVE-2015-8895 MLIST (link is external) BID (link is external) MISC (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	Integer truncation issue in coders/pict.c in ImageMagick before 7.0.5-0 allows remote attackers to cause a denial of service (application crash) via a crafted .pict file.	2017-03-15	4.3	CVE-2015-8896 MLIST (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) MISC (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	The SpliceImage function in MagickCore/transform.c in ImageMagick before 6.9.2-4 allows remote attackers to cause a denial of service (application crash) via a crafted png file.	2017-03-15	4.3	CVE-2015-8897 CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	The WriteImages function in magick/constitute.c in ImageMagick before 6.9.2-4 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted image file.	2017-03-15	4.3	CVE-2015-8898 MLIST (link is external) BID (link is external) CONFIRM (link is external) MISC (link is external)
intel_security_mcafee -- endpoint_security_web_control	Cross-site scripting vulnerability in Intel Security McAfee Endpoint Security (ENS) Web Control before 10.2.0.408.10 allows attackers to inject arbitrary web script or HTML via a crafted web site.	2017-03-14	4.3	CVE-2016-8011 CONFIRM (link is external)
jasper_project -- jasper	The jpc_tsfb_synthesize function in jpc_tsfb.c in JasPer before 1.900.9 allows remote attackers to	2017-03-15	5.0	CVE-2016-10248

	cause a denial of service (NULL pointer dereference) via vectors involving an empty sequence.			MISC CONFIRM (link is external)
jasper_project -- jasper	Integer overflow in the jpc_dec_tiledecode function in jpc_dec.c in JasPer before 1.900.12 allows remote attackers to have unspecified impact via a crafted image file, which triggers a heap-based buffer overflow.	2017-03-15	6.8	CVE-2016-10249 MISC CONFIRM (link is external)
jasper_project -- jasper	The jp2_colr_destroy function in jp2_cod.c in JasPer before 1.900.13 allows remote attackers to cause a denial of service (NULL pointer dereference) by leveraging incorrect cleanup of JP2 box data on error. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8887.	2017-03-15	5.0	CVE-2016-10250 MISC CONFIRM (link is external)
jasper_project -- jasper	Integer overflow in the jpc_pi_nextcprl function in jpc_t2cod.c in JasPer before 1.900.20 allows remote attackers to have unspecified impact via a crafted file, which triggers use of an uninitialized value.	2017-03-15	6.8	CVE-2016-10251 MISC CONFIRM (link is external)
jasper_project -- jasper	The jas_matrix_asl function in jas_seq.c in JasPer 1.900.27 allows remote attackers to cause a denial of service (invalid memory read and crash) via a crafted image.	2017-03-16	4.3	CVE-2017-5505 MLIST (link is external) MLIST (link is external) BID (link is external) MISC
jasper_project -- jasper	The jp2_cdef_destroy function in jp2_cod.c in JasPer before 2.0.13 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted image.	2017-03-15	4.3	CVE-2017-6850 MISC CONFIRM (link is external) CONFIRM (link is external)
jasper_project -- jasper	The jas_matrix_bindsub function in jas_seq.c in JasPer 2.0.10 allows remote attackers to cause a denial of service (invalid read) via a crafted image.	2017-03-15	4.3	CVE-2017-6851 MISC MISC (link is external)
jasper_project -- jasper	Heap-based buffer overflow in the jpc_dec_decodepkt function in jpc_t2dec.c in JasPer 2.0.10 allows remote attackers to have unspecified impact via a crafted image.	2017-03-15	6.8	CVE-2017-6852 MISC MISC (link is external)
jquery -- jquery-ui	Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject	2017-03-15	4.3	CVE-2016-7103 REDHAT (link is external)

	arbitrary web script or HTML via the closeText parameter of the dialog function.			CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) MISC (link is external)
keekoonvision -- kk002_ip_camera_firmware	Keekoon KK002 devices 1.8.12 HD have a Cross Site Request Forgery Vulnerability affecting goform/formChnUserPwd and goform/formUserMng (and the entire set of other pages).	2017-03-13	6.8	CVE-2017-6180 MISC (link is external)
lg_project -- lg	Cross-site scripting (XSS) vulnerability in lg.cgi in Cougar LG 1.9 allows remote attackers to inject arbitrary web script or HTML via the "addr" parameter.	2017-03-13	4.3	CVE-2014-3926 MISC (link is external) MISC (link is external) CONFIRM (link is external) MISC (link is external) MISC (link is external)
libgd -- libgd	The gdImageCreateFromGd2Ctx function in gd_gd2.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to cause a denial of service (application crash) via a crafted image file.	2017-03-15	4.3	CVE-2016-10167 CONFIRM (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
libgd -- libgd	Integer overflow in gd_io.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to have unspecified impact via vectors involving the number of horizontal and vertical chunks in an image.	2017-03-15	6.8	CVE-2016-10168 CONFIRM (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link

				is external)
libgd -- libgd	The read_image_tga function in gd_tga.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TGA file, related to the decompression buffer.	2017-03-15	4.3	CVE-2016-6906 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
libplist_project -- libplist	Heap-based buffer overflow in the parse_unicode_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (out-of-bounds write) and possibly code execution via a crafted plist file.	2017-03-15	4.4	CVE-2017-6438 MISC (link is external)
linux -- linux_kernel	Race condition in kernel/ucount.c in the Linux kernel through 4.10.2 allows local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via crafted system calls that leverage certain decrement behavior that causes incorrect interaction between put_ucounts and get_ucounts.	2017-03-14	6.9	CVE-2017-6874 CONFIRM BID (link is external) CONFIRM (link is external)
lutim_project -- lutim	Cross-site scripting (XSS) vulnerability in SVG file handling in Lutim 0.7.1 and earlier allows remote attackers to inject arbitrary web script.	2017-03-14	4.3	CVE-2017-6877 BID (link is external) CONFIRM CONFIRM
mangoswebv4_project -- mangoswebv4	paintballrefjosh/MaNGOSWebV4 4.0.8 is vulnerable to a reflected XSS in inc/admin/template_files/admin.faq.php (id parameter).	2017-03-11	4.3	CVE-2017-6808 BID (link is external) CONFIRM (link is external)
mangoswebv4_project -- mangoswebv4	paintballrefjosh/MaNGOSWebV4 4.0.8 is vulnerable to a reflected XSS in inc/admin/template_files/admin.donate.php (id parameter).	2017-03-11	4.3	CVE-2017-6809 BID (link is external) CONFIRM (link is external)
mangoswebv4_project -- mangoswebv4	paintballrefjosh/MaNGOSWebV4 4.0.8 is vulnerable to a reflected XSS in inc/admin/template_files/admin.fplinks.php (linkid parameter).	2017-03-11	4.3	CVE-2017-6810 BID (link is external) CONFIRM (link is external)
mangoswebv4_project -- mangoswebv4	paintballrefjosh/MaNGOSWebV4 4.0.8 is vulnerable to a reflected XSS in	2017-03-11	4.3	CVE-2017-6811 BID (link is external)

	inc/admin/template_files/admin.shop.php (id parameter).			CONFIRM (link is external)
mangoswebv4_project -- mangoswebv4	paintballrefjosh/MaNGOSWebV4 4.0.8 is vulnerable to a reflected XSS in inc/admin/template_files/admin.vote.php (id parameter).	2017-03-11	4.3	CVE-2017-6812 BID (link is external) CONFIRM (link is external)
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in view_filters_page.php in MantisBT before 2.2.1 allows remote attackers to inject arbitrary JavaScript via the 'view_type' parameter.	2017-03-10	4.3	CVE-2017-6799 CONFIRM CONFIRM (link is external) BID (link is external) CONFIRM (link is external)
mcafee -- virusscan_enterprise	Special element injection vulnerability in Intel Security VirusScan Enterprise Linux (VSEL) 2.0.3 (and earlier) allows authenticated remote attackers to read files on the webserver via a crafted user input.	2017-03-14	4.0	CVE-2016-8017 BID (link is external) CONFIRM (link is external)
mcafee -- virusscan_enterprise	Cross-site request forgery (CSRF) vulnerability in Intel Security VirusScan Enterprise Linux (VSEL) 2.0.3 (and earlier) allows authenticated remote attackers to execute unauthorized commands via a crafted user input.	2017-03-14	6.0	CVE-2016-8018 BID (link is external) CONFIRM (link is external)
mcafee -- virusscan_enterprise	Cross-site scripting (XSS) vulnerability in attributes in Intel Security VirusScan Enterprise Linux (VSEL) 2.0.3 (and earlier) allows unauthenticated remote attackers to inject arbitrary web script or HTML via a crafted user input.	2017-03-14	4.3	CVE-2016-8019 BID (link is external) CONFIRM (link is external)
mcafee -- virusscan_enterprise	Improper control of generation of code vulnerability in Intel Security VirusScan Enterprise Linux (VSEL) 2.0.3 (and earlier) allows remote authenticated users to execute arbitrary code via a crafted HTTP request parameter.	2017-03-14	6.0	CVE-2016-8020 BID (link is external) CONFIRM (link is external)
mcafee -- virusscan_enterprise	Authentication bypass by spoofing vulnerability in Intel Security VirusScan Enterprise Linux (VSEL) 2.0.3 (and earlier) allows remote unauthenticated attacker to execute arbitrary code or cause a denial of service via a crafted authentication cookie.	2017-03-14	5.1	CVE-2016-8022 BID (link is external) CONFIRM (link is external)

mcafee -- virusscan_enterprise	Authentication bypass by assumed-immutable data vulnerability in Intel Security VirusScan Enterprise Linux (VSEL) 2.0.3 (and earlier) allows remote unauthenticated attacker to bypass server authentication via a crafted authentication cookie.	2017-03-14	6.8	CVE-2016-8023 BID (link is external) CONFIRM (link is external)
mcafee -- virusscan_enterprise	Improper neutralization of CRLF sequences in HTTP headers vulnerability in Intel Security VirusScan Enterprise Linux (VSEL) 2.0.3 (and earlier) allows remote unauthenticated attacker to obtain sensitive information via the server HTTP response spoofing.	2017-03-14	6.8	CVE-2016-8024 BID (link is external) CONFIRM (link is external)
mcafee -- virusscan_enterprise	SQL injection vulnerability in Intel Security VirusScan Enterprise Linux (VSEL) 2.0.3 (and earlier) allows remote authenticated users to obtain product information via a crafted HTTP request parameter.	2017-03-14	6.0	CVE-2016-8025 BID (link is external) CONFIRM (link is external)
microsoft -- edge	Microsoft Edge allows remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Edge Information Disclosure Vulnerability." This vulnerability is different from those described in CVE-2017-0009, CVE-2017-0017, CVE-2017-0065, and CVE-2017-0068.	2017-03-16	4.3	CVE-2017-0011 BID (link is external) CONFIRM (link is external)
microsoft -- edge	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to spoof web content via a crafted web site, aka "Microsoft Browser Spoofing Vulnerability." This vulnerability is different from those described in CVE-2017-0033 and CVE-2017-0069.	2017-03-16	4.3	CVE-2017-0012 BID (link is external) CONFIRM (link is external)
microsoft -- edge	The RegEx class in the XSS filter in Microsoft Edge allows remote attackers to conduct cross-site scripting (XSS) attacks and obtain sensitive information via unspecified vectors, aka "Microsoft Edge Information Disclosure Vulnerability." This vulnerability is different from those described in CVE-2017-0009, CVE-2017-0011, CVE-2017-0065, and CVE-2017-0068.	2017-03-16	4.3	CVE-2017-0017 BID (link is external) CONFIRM (link is external)
microsoft -- edge	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to spoof web content via a	2017-03-16	4.3	CVE-2017-0033 BID (link is external)

	crafted web site, aka "Microsoft Browser Spoofing Vulnerability." This vulnerability is different from those described in CVE-2017-0012 and CVE-2017-0069.			CONFIRM (link is external)
microsoft -- edge	Microsoft Edge allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability." This vulnerability is different from those described in CVE-2017-0009, CVE-2017-0011, CVE-2017-0017, and CVE-2017-0068.	2017-03-16	4.3	CVE-2017-0065 BID (link is external) CONFIRM (link is external)
microsoft -- edge	Browsers in Microsoft Edge allow remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Microsoft Edge Information Disclosure Vulnerability." This vulnerability is different from those described in CVE-2017-0009, CVE-2017-0011, CVE-2017-0017, and CVE-2017-0065.	2017-03-16	4.3	CVE-2017-0068 BID (link is external) CONFIRM (link is external)
microsoft -- edge	Microsoft Edge allows remote attackers to spoof web content via a crafted web site, aka "Microsoft Edge Spoofing Vulnerability." This vulnerability is different from those described in CVE-2017-0012 and CVE-2017-0033.	2017-03-16	4.3	CVE-2017-0069 BID (link is external) CONFIRM (link is external)
microsoft -- edge	Microsoft Edge allows remote attackers to bypass the Same Origin Policy for HTML elements in other browser windows, aka "Microsoft Edge Security Feature Bypass Vulnerability." This vulnerability is different from those described in CVE-2017-0066 and CVE-2017-0140.	2017-03-16	4.0	CVE-2017-0135 BID (link is external) CONFIRM (link is external)
microsoft -- edge	Microsoft Edge allows remote attackers to bypass the Same Origin Policy for HTML elements in other browser windows, aka "Microsoft Edge Security Feature Bypass Vulnerability." This vulnerability is different from those described in CVE-2017-0066 and CVE-2017-0135.	2017-03-16	4.0	CVE-2017-0140 BID (link is external) CONFIRM (link is external)
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allow remote attackers to obtain sensitive information from process memory via a crafted web site, aka	2017-03-16	4.3	CVE-2017-0008 BID (link is external) CONFIRM (link

	"Internet Explorer Information Disclosure Vulnerability." This vulnerability is different from those described in CVE-2017-0009 and CVE-2017-0059.			is external)
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allow remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability." This vulnerability is different from those described in CVE-2017-0011, CVE-2017-0017, CVE-2017-0065, and CVE-2017-0068.	2017-03-16	4.3	CVE-2017-0009 BID (link is external) CONFIRM (link is external)
microsoft -- internet_explorer	The VBScript engine in Microsoft Internet Explorer 11 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Scripting Engine Information Disclosure Vulnerability." This vulnerability is different from those described in CVE-2017-0018, and CVE-2017-0037.	2017-03-16	4.3	CVE-2017-0049 BID (link is external) CONFIRM (link is external)
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allow remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability." This vulnerability is different from those described in CVE-2017-0008 and CVE-2017-0009.	2017-03-16	4.3	CVE-2017-0059 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka "Uniscribe Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089, and CVE-2017-0090.	2017-03-16	6.8	CVE-2017-0072 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web	2017-03-16	4.3	CVE-2017-0085 BID (link is external) CONFIRM (link is external)

	site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.			
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.	2017-03-16	4.3	CVE-2017-0091 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.	2017-03-16	4.3	CVE-2017-0092 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web	2017-03-16	4.3	CVE-2017-0111 BID (link is external) CONFIRM (link is external)

	site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.			
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.	2017-03-16	4.3	CVE-2017-0112 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.	2017-03-16	4.3	CVE-2017-0113 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web	2017-03-16	4.3	CVE-2017-0114 BID (link is external) CONFIRM (link is external)

	site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.			
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.	2017-03-16	4.3	CVE-2017-0115 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.	2017-03-16	4.3	CVE-2017-0116 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web	2017-03-16	4.3	CVE-2017-0117 BID (link is external) CONFIRM (link is external)

	site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.			
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.	2017-03-16	4.3	CVE-2017-0119 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Windows Uniscribe Information Disclosure Vulnerability."	2017-03-16	4.3	CVE-2017-0120 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125,	2017-03-16	4.3	CVE-2017-0122 BID (link is external) CONFIRM (link is external)

	CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.			
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.	2017-03-16	4.3	CVE-2017-0123 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.	2017-03-16	4.3	CVE-2017-0124 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124,	2017-03-16	4.3	CVE-2017-0125 BID (link is external) CONFIRM (link is external)

	CVE-2017-0126, CVE-2017-0127, and CVE-2017-0128.			
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0127, and CVE-2017-0128.	2017-03-16	4.3	CVE-2017-0126 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124, CVE-2017-0125, CVE-2017-0126, and CVE-2017-0128.	2017-03-16	4.3	CVE-2017-0127 BID (link is external) CONFIRM (link is external)
microsoft -- windows_vista	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE-2017-0085, CVE-2017-0091, CVE-2017-0092, CVE-2017-0111, CVE-2017-0112, CVE-2017-0113, CVE-2017-0114, CVE-2017-0115, CVE-2017-0116, CVE-2017-0117, CVE-2017-0118, CVE-2017-0119, CVE-2017-0120, CVE-2017-0121, CVE-2017-0122, CVE-2017-0123, CVE-2017-0124,	2017-03-16	4.3	CVE-2017-0128 BID (link is external) CONFIRM (link is external)

	CVE-2017-0125, CVE-2017-0126, and CVE-2017-0127.			
netpbm -- netpbm	tiffttopnm in netpbm 10.47.63 does not properly use the libtiff TIFFRGBAImageGet function, which allows remote attackers to cause a denial of service (out-of-bounds read and write) via a crafted tiff image file, related to transposing width and height values.	2017-03-15	4.3	CVE-2017-5849 MISC MISC MLIST (link is external) BID (link is external) FEDORA FEDORA
open_edx -- edx-platform	Open edX edx-platform before 2015-08-25 requires use of the database for storage of SAML SSO secrets, which makes it easier for context-dependent attackers to obtain sensitive information by leveraging access to a database backup.	2017-03-13	4.3	CVE-2015-6671 CONFIRM (link is external) CONFIRM
paloaltonetworks -- pan-os	The Management Web Interface in Palo Alto Networks PAN-OS before 6.1.16, 7.0.x before 7.0.13, and 7.1.x before 7.1.8 allows remote authenticated users to read arbitrary files via unspecified vectors.	2017-03-15	4.0	CVE-2017-5583 BID (link is external) SECTRACK (link is external) CONFIRM (link is external)
partclone_project -- partclone	partclone.chkimg in partclone 0.2.89 is prone to a heap-based buffer overflow vulnerability due to insufficient validation of the partclone image header. An attacker may be able to launch a 'Denial of Service attack' in the context of the user running the affected application.	2017-03-10	4.3	CVE-2017-6596 MISC (link is external)
pharos -- popup	A denial of service vulnerability exists in the psnotifyd application of the Pharos PopUp printer client version 9.0. A specially crafted packet can be sent to the victim's computer and can lead to an out of bounds read causing a crash and a denial of service.	2017-03-10	5.0	CVE-2017-2786 BID (link is external) MISC (link is external)
podofo_project -- podofo	The ColorChanger::GetColorFromStack function in colorchanger.cpp in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (invalid read) via a crafted file.	2017-03-15	4.3	CVE-2017-6840 MISC
podofo_project --	The	2017-03-15	4.3	CVE-2017-6841 MISC

podofo	GraphicsStack::TGraphicsStackElement::~TGraphicsStackElement function in graphicsstack.h in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.			
podofo_project -- podofo	The ColorChanger::GetColorFromStack function in colorchanger.cpp in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.	2017-03-15	4.3	CVE-2017-6842 MISC
podofo_project -- podofo	Heap-based buffer overflow in the PoDoFo::PdfVariant::DelayedLoad function in PdfVariant.h in PoDoFo 0.9.4 allows remote attackers to have unspecified impact via a crafted file.	2017-03-15	6.8	CVE-2017-6843 MISC
podofo_project -- podofo	Buffer overflow in the PoDoFo::PdfParser::ReadXRefSubsection function in PdfParser.cpp in PoDoFo 0.9.4 allows remote attackers to have unspecified impact via a crafted file.	2017-03-15	6.8	CVE-2017-6844 MISC
podofo_project -- podofo	The PoDoFo::PdfColor::operator function in PdfColor.cpp in PoDoFo 0.9.4 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.	2017-03-15	4.3	CVE-2017-6845 MISC
podofo_project -- podofo	The GraphicsStack::TGraphicsStackElement::SetNonStrokingColorSpace function in graphicsstack.h in PoDoFo 0.9.4 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.	2017-03-15	4.3	CVE-2017-6846 MISC
podofo_project -- podofo	The PoDoFo::PdfVariant::DelayedLoad function in PdfVariant.h in PoDoFo 0.9.4 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.	2017-03-15	4.3	CVE-2017-6847 MISC
podofo_project -- podofo	The PoDoFo::PdfXObject::PdfXObject function in PdfXObject.cpp in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.	2017-03-15	4.3	CVE-2017-6848 MISC
podofo_project --	The PoDoFo::PdfColorGray::~PdfColorGray function	2017-03-15	4.3	CVE-2017-6849 MISC

podofo	in PdfColor.cpp in PoDoFo 0.9.4 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.			
qemu -- qemu	Memory leak in hw/watchdog/wdt_i6300esb.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption and QEMU process crash) via a large number of device unplug operations.	2017-03-15	4.9	CVE-2016-10155 CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)
qemu -- qemu	Memory leak in hw/audio/ac97.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption and QEMU process crash) via a large number of device unplug operations.	2017-03-15	4.9	CVE-2017-5525 CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)
qemu -- qemu	Memory leak in hw/audio/es1370.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption and QEMU process crash) via a large number of device unplug operations.	2017-03-15	4.9	CVE-2017-5526 CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)
qemu -- qemu	Memory leak in the virgl_resource_attach_backing function in hw/display/virtio-gpu-3d.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (host memory consumption) via a large number of VIRTIO_GPU_CMD_RESOURCE_ATTACH_BACKING commands.	2017-03-15	4.9	CVE-2017-5552 CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)
qemu -- qemu	Memory leak in the virtio_gpu_resource_attach_backing function in hw/display/virtio-gpu.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (host memory consumption) via a large number of VIRTIO_GPU_CMD_RESOURCE_ATTACH_BACKING commands.	2017-03-15	4.9	CVE-2017-5578 CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)
qemu -- qemu	Memory leak in the serial_exit_core function in	2017-03-15	4.9	CVE-2017-5579

	hw/char/serial.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption and QEMU process crash) via a large number of device unplug operations.			CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)
qemu -- qemu	Memory leak in the megasas_handle_dcmd function in hw/scsi/megasas.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption) via MegaRAID Firmware Interface (MFI) commands with the sglist size set to a value over 2 Gb.	2017-03-16	4.9	CVE-2017-5856 CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
qemu -- qemu	Memory leak in the virgl_cmd_resource_unref function in hw/display/virtio-gpu-3d.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (host memory consumption) via a large number of VIRTIO_GPU_CMD_RESOURCE_UNREF commands sent without detaching the backing storage beforehand.	2017-03-16	4.9	CVE-2017-5857 CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
r_project -- r	An exploitable buffer overflow vulnerability exists in the LoadEncoding functionality of the R programming language version 3.3.0. A specially crafted R script can cause a buffer overflow resulting in a memory corruption. An attacker can send a malicious R script to trigger this vulnerability.	2017-03-10	6.8	CVE-2016-8714 BID (link is external) MISC (link is external)
roundcube -- roundcube_webmail	rcube_utils.php in Roundcube before 1.1.8 and 1.2.x before 1.2.4 is susceptible to a cross-site scripting vulnerability via a crafted Cascading Style Sheets (CSS) token sequence within an SVG element.	2017-03-12	4.3	CVE-2017-6820 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link

				is external)
sap -- businessobjects_financial_consolidation	Cross-site scripting (XSS) vulnerability in the help component of SAP BusinessObjects Financial Consolidation 10.0.0.1933 allows remote attackers to inject arbitrary web script or HTML via a GET request. /finance/help/en/frameset.htm is the URI for this component. The vendor response is SAP Security Note 2368106.	2017-03-16	4.3	CVE-2017-6061 MISC (link is external) MISC BID (link is external) SECTRACK (link is external)
softaculous -- whmcs_reseller_module	The WHMCS Reseller Module V2 2.0.2 in Softaculous Virtualizor before 2.9.1.0 does not verify the user correctly, which allows remote authenticated users to control other virtual machines managed by Virtualizor by accessing a modified URL.	2017-03-11	6.5	CVE-2017-6513 CONFIRM (link is external)
telegram -- messenger	An issue was discovered in Telegram Messenger 2.6 for iOS and 1.8.2 for Android. Secret chat messages are available in cleartext in process memory and a .db file.	2017-03-14	5.0	CVE-2014-8688 MISC (link is external)
uninett -- mod_auth_mellon	mod_auth_mellon before 0.13.1 is vulnerable to a Cross-Site Session Transfer attack, where a user with access to one web site running on a server can copy their session cookie to a different web site on the same server to get access to that site.	2017-03-13	4.3	CVE-2017-6807 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
viewvc -- viewvc	Cross-site scripting (XSS) vulnerability in the nav_path function in lib/viewvc.py in ViewVC before 1.1.26 allows remote attackers to inject arbitrary web script or HTML via the nav_data name.	2017-03-15	4.3	CVE-2017-5938 SUSE DEBIAN MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
virglrenderer_project -- virglrenderer	Memory leak in the vrend_renderer_context_create_internal function in vrend_decode.c in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (host memory consumption) by repeatedly creating a decode context.	2017-03-15	4.9	CVE-2016-10163 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM MLIST

virglrenderer_project -- virglrenderer	Memory leak in the vrend_renderer_init_blit_ctx function in vrend_blitter.c in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (host memory consumption) via a large number of VIRGL_CCMD_BLIT commands.	2017-03-15	4.9	CVE-2017-5993 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM MLIST
virglrenderer_project -- virglrenderer	Memory leak in the add_shader_program function in vrend_renderer.c in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (host memory consumption) via vectors involving the sprog variable.	2017-03-15	4.9	CVE-2017-6317 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM MLIST
virglrenderer_project -- virglrenderer	Memory leak in the vrend_create_vertex_elements_state function in vrend_renderer.c in virglrenderer allows local guest OS users to cause a denial of service (host memory consumption) via a large number of VIRGL_OBJECT_VERTEX_ELEMENTS commands.	2017-03-15	4.9	CVE-2017-6386 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM
wavpack_project -- wavpack	The read_code function in read_words.c in Wavpack before 5.1.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WV file.	2017-03-14	4.3	CVE-2016-10169 MLIST (link is external) BID (link is external) CONFIRM (link is external) MISC (link is external)
wavpack_project -- wavpack	The WriteCaffHeader function in cli/caff.c in Wavpack before 5.1.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WV file.	2017-03-14	4.3	CVE-2016-10170 MLIST (link is external) BID (link is external) CONFIRM (link is external) MISC (link is external)
wavpack_project -- wavpack	The unreorder_channels function in cli/wvunpack.c in Wavpack before 5.1.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a	2017-03-14	4.3	CVE-2016-10171 MLIST (link is external)

	crafted WV file.			BID (link is external) CONFIRM (link is external) MISC (link is external)
wavpack_project -- wavpack	The read_new_config_info function in open_utils.c in Wavpack before 5.1.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WV file.	2017-03-14	4.3	CVE-2016-10172 MLIST (link is external) BID (link is external) CONFIRM (link is external) MISC (link is external)
wordpress -- wordpress	In WordPress before 4.7.3 (wp-includes/pluggable.php), control characters can trick redirect URL validation.	2017-03-11	5.8	CVE-2017-6815 BID (link is external) MISC MISC (link is external) MISC
wordpress -- wordpress	In WordPress before 4.7.3 (wp-admin/plugins.php), unintended files can be deleted by administrators using the plugin deletion functionality.	2017-03-11	4.0	CVE-2017-6816 BID (link is external) MISC MISC (link is external) MISC
wordpress -- wordpress	In WordPress before 4.7.3 (wp-admin/js/tags-box.js), there is cross-site scripting (XSS) via taxonomy term names.	2017-03-11	4.3	CVE-2017-6818 BID (link is external) MISC MISC (link is external) MISC
wordpress -- wordpress	In WordPress before 4.7.3, there is cross-site request forgery (CSRF) in Press This (wp-admin/includes/class-wp-press-this.php), leading to excessive use of server resources. The CSRF can trigger an outbound HTTP request for a large file that is then parsed by Press This.	2017-03-11	4.3	CVE-2017-6819 MISC (link is external) BID (link is external) MISC MISC (link is external) MISC (link is external) MISC
ytnef_project --	An issue was discovered in ytnef before 1.9.2. An	2017-03-10	5.0	CVE-2017-6800

ytnef	invalid memory access (heap-based buffer over-read) can occur during handling of LONG data types, related to MAPIPrint() in libytnef.			CONFIRM (link is external) CONFIRM (link is external)
ytnef_project -- ytnef	An issue was discovered in ytnef before 1.9.2. There is a potential out-of-bounds access with fields of Size 0 in TNEFParse() in libytnef.	2017-03-10	5.0	CVE-2017-6801 CONFIRM (link is external)
ytnef_project -- ytnef	An issue was discovered in ytnef before 1.9.2. There is a potential heap-based buffer over-read on incoming Compressed RTF Streams, related to DecompressRTF() in libytnef.	2017-03-10	5.0	CVE-2017-6802 CONFIRM (link is external) CONFIRM (link is external)
zahmit_design -- connections_business_directory_plugin	Cross-site scripting (XSS) vulnerability in includes/admin/pages/manage.php in the Connections Business Directory plugin before 8.5.9 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s variable.	2017-03-16	4.3	CVE-2016-0770 MLIST (link is external) BID (link is external) MISC (link is external) CONFIRM
zammad -- zammad	An XSS issue was discovered in Zammad before 1.0.4, 1.1.x before 1.1.3, and 1.2.x before 1.2.1. Attachments are opened in a new tab instead of getting downloaded. This creates an attack vector of executing code in the domain of the application.	2017-03-13	4.3	CVE-2017-5620 BID (link is external) CONFIRM (link is external)
zammad -- zammad	An issue was discovered in Zammad before 1.0.4, 1.1.x before 1.1.3, and 1.2.x before 1.2.1. XSS can be triggered via malicious HTML in a chat message or the content of a ticket article, when using either the REST API or the WebSocket API.	2017-03-13	4.3	CVE-2017-5621 BID (link is external) CONFIRM (link is external)
zammad -- zammad	A CSRF issue was discovered in Zammad before 1.0.4, 1.1.x before 1.1.3, and 1.2.x before 1.2.1. To exploit the vulnerability, an attacker can send cross-domain requests directly to the REST API for users with a valid session cookie.	2017-03-13	6.8	CVE-2017-6081 BID (link is external) CONFIRM (link is external)

Low Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
busybox -- busybox	The add_probe function in modutils/modprobe.c in BusyBox before 1.23.0 allows local users to bypass intended restrictions on loading kernel modules via a / (slash) character in a module name, as demonstrated by an "ifconfig /usbserial up" command or a "mount -t /snd_pcm none /" command.	2017-03-12	2.1	CVE-2014-9645 CONFIRM (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) MISC (link is external)
foxitsoftware -- phantompdf	The ConvertToPDF plugin in Foxit Reader before 8.2.1 and PhantomPDF before 8.2.1 on Windows, when the gflags app is enabled, allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted TIFF image. The vulnerability could lead to information disclosure; an attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process.	2017-03-14	2.6	CVE-2017-6883 BID (link is external) MISC (link is external) CONFIRM (link is external)
libplist_project -- libplist	The parse_string_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (memory corruption) via a crafted plist file.	2017-03-15	1.9	CVE-2017-6435 CONFIRM (link is external) MISC (link is external)
libplist_project -- libplist	The parse_string_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (memory allocation error) via a crafted plist file.	2017-03-15	1.9	CVE-2017-6436 CONFIRM (link is external) MISC (link is external)
libplist_project -- libplist	The base64encode function in base64.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (out-of-bounds read) via a crafted plist file.	2017-03-15	1.9	CVE-2017-6437 MISC (link is external)
libplist_project -- libplist	Heap-based buffer overflow in the parse_string_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to	2017-03-15	1.9	CVE-2017-6439 CONFIRM (link is external)

	cause a denial of service (out-of-bounds write) via a crafted plist file.			MISC (link is external)
libplist_project -- libplist	The parse_data_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (memory allocation error) via a crafted plist file.	2017-03-15	1.9	CVE-2017-6440 MISC (link is external)
mcafee -- application_control	A write protection and execution bypass vulnerability in McAfee (now Intel Security) Application Control (MAC) 6.1.0 for Linux and earlier allows authenticated users to change binaries that are part of the Application Control whitelist and allows execution of binaries via specific conditions.	2017-03-14	2.1	CVE-2013-7460 CONFIRM (link is external)
mcafee -- application_control	A write protection and execution bypass vulnerability in McAfee (now Intel Security) Change Control (MCC) 6.1.0 for Linux and earlier allows authenticated users to change files that are part of write protection rules via specific conditions.	2017-03-14	2.1	CVE-2013-7461 CONFIRM (link is external)
mcafee -- virusscan_enterprise	Information exposure in Intel Security VirusScan Enterprise Linux (VSEL) 2.0.3 (and earlier) allows authenticated remote attackers to obtain the existence of unauthorized files on the system via a URL parameter.	2017-03-14	3.5	CVE-2016-8016 BID (link is external) CONFIRM (link is external)
mcafee -- virusscan_enterprise	Improper verification of cryptographic signature vulnerability in Intel Security VirusScan Enterprise Linux (VSEL) 2.0.3 (and earlier) allows remote authenticated users to spoof update server and execute arbitrary code via a crafted input file.	2017-03-14	3.5	CVE-2016-8021 BID (link is external) CONFIRM (link is external)
microsoft -- windows_10	Microsoft Windows 10 1607 and Windows Server 2016 allow remote attackers to cause a denial of service (application hang) via a crafted Office document, aka "Microsoft Hyper-V Network Switch Denial of Service Vulnerability." This vulnerability is different from those described in CVE-2017-0074, CVE-2017-0076, CVE-2017-0097, CVE-2017-0098, and CVE-2017-0099.	2017-03-16	2.9	CVE-2017-0051 BID (link is external) CONFIRM (link is external)
paloaltonetworks -- pan-os	Cross-site scripting (XSS) vulnerability in the Management Web Interface in Palo Alto Networks PAN-OS 5.1, 6.x before 6.1.16, 7.0.x before 7.0.13,	2017-03-15	3.5	CVE-2017-5584 CONFIRM (link is external) BID (link is

	and 7.1.x before 7.1.8 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.			external) SECTRACK (link is external)
qemu -- qemu	The sdhci_sdma_transfer_multi_blocks function in hw/sd/sdhci.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (out-of-bounds heap access and crash) or execute arbitrary code on the QEMU host via vectors involving the data transfer length.	2017-03-16	2.1	CVE-2017-5667 CONFIRM MLIST (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
qemu -- qemu	The ohci_service_ed_list function in hw/usb/hcd-ohci.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (infinite loop) via vectors involving the number of link endpoint list descriptors.	2017-03-15	2.1	CVE-2017-6505 CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external)
suse -- linux_enterprise_server	Integer overflow in the emulated_apdu_from_guest function in usb/dev-smartcard-reader.c in Quick Emulator (Qemu), when built with the CCID Card device emulator support, allows local users to cause a denial of service (application crash) via a large Application Protocol Data Units (APDU) unit.	2017-03-15	2.1	CVE-2017-5898 CONFIRM SUSE SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external) GENTOO
virglrenderer_project -- virglrenderer	The parse_instruction function in gallium/auxiliary/tgsi/tgsi_text.c in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (out-of-bounds array access and process crash) via a crafted texture instruction.	2017-03-15	2.1	CVE-2017-5580 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM MLIST
virglrenderer_project -- virglrenderer	The util_format_is_pure_uint function in vrend_renderer.c in Virgil 3d project (aka virglrenderer) 0.6.0 and earlier allows local guest OS users to cause a denial of service (NULL pointer	2017-03-15	2.1	CVE-2017-5937 MLIST (link is external) BID (link is external) CONFIRM (link

	dereference) via a crafted VIRGL_CCMD_CLEAR command.			is external) CONFIRM
virglrenderer_project -- virglrenderer	Stack-based buffer overflow in the vrend_decode_set_framebuffer_state function in vrend_decode.c in virglrenderer before 926b9b3460a48f6454d8bbe9e44313d86a65447f, as used in Quick Emulator (QEMU), allows a local guest users to cause a denial of service (application crash) via the "nr_cbufs" argument.	2017-03-14	2.1	CVE-2017-5957 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM
virglrenderer_project -- virglrenderer	Heap-based buffer overflow in the vrend_create_vertex_elements_state function in vrend_renderer.c in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (out-of-bounds array access and crash) via the num_elements parameter.	2017-03-15	2.1	CVE-2017-5994 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM MLIST
virglrenderer_project -- virglrenderer	Stack-based buffer overflow in the parse_identifier function in tgsi_text.c in the TGSI auxiliary module in the Gallium driver in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (out-of-bounds array access and QEMU process crash) via vectors related to parsing properties.	2017-03-15	2.1	CVE-2017-6209 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM MLIST
virglrenderer_project -- virglrenderer	The vrend_decode_reset function in vrend_decode.c in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (NULL pointer dereference and QEMU process crash) by destroying context 0 (zero).	2017-03-15	2.1	CVE-2017-6210 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM MLIST
wordpress -- wordpress	In WordPress before 4.7.3, there is authenticated Cross-Site Scripting (XSS) via Media File Metadata. This is demonstrated by both (1) mishandling of the playlist shortcode in the wp_playlist_shortcode function in wp-includes/media.php and (2) mishandling of meta information in the renderTracks function in wp-includes/js/mediaelement/wp-playlist.js.	2017-03-11	3.5	CVE-2017-6814 MISC (link is external) BID (link is external) MISC MISC (link is external) MISC (link is external) MISC

wordpress -- wordpress	In WordPress before 4.7.3 (wp-includes/embed.php), there is authenticated Cross-Site Scripting (XSS) in YouTube URL Embeds.	2017-03-11	3.5	CVE-2017-6817 BID (link is external) MISC MISC (link is external) MISC
busybox -- busybox	The add_probe function in modutils/modprobe.c in BusyBox before 1.23.0 allows local users to bypass intended restrictions on loading kernel modules via a / (slash) character in a module name, as demonstrated by an "ifconfig /usbserial up" command or a "mount -t /snd_pcm none /" command.	2017-03-12	2.1	CVE-2014-9645 CONFIRM (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) MISC (link is external)
foxitsoftware -- phantompdf	The ConvertToPDF plugin in Foxit Reader before 8.2.1 and PhantomPDF before 8.2.1 on Windows, when the gflags app is enabled, allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted TIFF image. The vulnerability could lead to information disclosure; an attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process.	2017-03-14	2.6	CVE-2017-6883 BID (link is external) MISC (link is external) CONFIRM (link is external)
libplist_project -- libplist	The parse_string_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (memory corruption) via a crafted plist file.	2017-03-15	1.9	CVE-2017-6435 CONFIRM (link is external) MISC (link is external)
libplist_project -- libplist	The parse_string_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (memory allocation error) via a crafted plist file.	2017-03-15	1.9	CVE-2017-6436 CONFIRM (link is external) MISC (link is external)
libplist_project -- libplist	The base64encode function in base64.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (out-of-bounds read) via a crafted plist file.	2017-03-15	1.9	CVE-2017-6437 MISC (link is external)
libplist_project -- libplist	Heap-based buffer overflow in the parse_string_node function in bplist.c in	2017-03-15	1.9	CVE-2017-6439 CONFIRM (link

	libimobiledevice libplist 1.12 allows local users to cause a denial of service (out-of-bounds write) via a crafted plist file.			is external) MISC (link is external)
libplist_project -- libplist	The parse_data_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (memory allocation error) via a crafted plist file.	2017-03-15	1.9	CVE-2017-6440 MISC (link is external)
mcafee -- application_control	A write protection and execution bypass vulnerability in McAfee (now Intel Security) Application Control (MAC) 6.1.0 for Linux and earlier allows authenticated users to change binaries that are part of the Application Control whitelist and allows execution of binaries via specific conditions.	2017-03-14	2.1	CVE-2013-7460 CONFIRM (link is external)
mcafee -- application_control	A write protection and execution bypass vulnerability in McAfee (now Intel Security) Change Control (MCC) 6.1.0 for Linux and earlier allows authenticated users to change files that are part of write protection rules via specific conditions.	2017-03-14	2.1	CVE-2013-7461 CONFIRM (link is external)
mcafee -- virusscan_enterprise	Information exposure in Intel Security VirusScan Enterprise Linux (VSEL) 2.0.3 (and earlier) allows authenticated remote attackers to obtain the existence of unauthorized files on the system via a URL parameter.	2017-03-14	3.5	CVE-2016-8016 BID (link is external) CONFIRM (link is external)
mcafee -- virusscan_enterprise	Improper verification of cryptographic signature vulnerability in Intel Security VirusScan Enterprise Linux (VSEL) 2.0.3 (and earlier) allows remote authenticated users to spoof update server and execute arbitrary code via a crafted input file.	2017-03-14	3.5	CVE-2016-8021 BID (link is external) CONFIRM (link is external)
microsoft -- windows_10	Microsoft Windows 10 1607 and Windows Server 2016 allow remote attackers to cause a denial of service (application hang) via a crafted Office document, aka "Microsoft Hyper-V Network Switch Denial of Service Vulnerability." This vulnerability is different from those described in CVE-2017-0074, CVE-2017-0076, CVE-2017-0097, CVE-2017-0098, and CVE-2017-0099.	2017-03-16	2.9	CVE-2017-0051 BID (link is external) CONFIRM (link is external)
paloaltonetworks -- pan-os	Cross-site scripting (XSS) vulnerability in the Management Web Interface in Palo Alto Networks	2017-03-15	3.5	CVE-2017-5584 CONFIRM (link

	PAN-OS 5.1, 6.x before 6.1.16, 7.0.x before 7.0.13, and 7.1.x before 7.1.8 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.			is external) BID (link is external) SECTRACK (link is external)
qemu -- qemu	The sdhci_sdma_transfer_multi_blocks function in hw/sd/sdhci.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (out-of-bounds heap access and crash) or execute arbitrary code on the QEMU host via vectors involving the data transfer length.	2017-03-16	2.1	CVE-2017-5667 CONFIRM MLIST (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
qemu -- qemu	The ohci_service_ed_list function in hw/usb/hcd-ohci.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (infinite loop) via vectors involving the number of link endpoint list descriptors.	2017-03-15	2.1	CVE-2017-6505 CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external)
suse -- linux_enterprise_server	Integer overflow in the emulated_apdu_from_guest function in usb/dev-smartcard-reader.c in Quick Emulator (Qemu), when built with the CCID Card device emulator support, allows local users to cause a denial of service (application crash) via a large Application Protocol Data Units (APDU) unit.	2017-03-15	2.1	CVE-2017-5898 CONFIRM SUSE SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external) GENTOO
virglrenderer_project -- virglrenderer	The parse_instruction function in gallium/auxiliary/tgsi/tgsi_text.c in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (out-of-bounds array access and process crash) via a crafted texture instruction.	2017-03-15	2.1	CVE-2017-5580 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM MLIST
virglrenderer_project -- virglrenderer	The util_format_is_pure_uint function in vrend_renderer.c in Virgil 3d project (aka virglrenderer) 0.6.0 and earlier allows local guest OS	2017-03-15	2.1	CVE-2017-5937 MLIST (link is external) BID (link is external)

	users to cause a denial of service (NULL pointer dereference) via a crafted VIRGL_CCMD_CLEAR command.			CONFIRM (link is external) CONFIRM
virglrenderer_project -- virglrenderer	Stack-based buffer overflow in the vrend_decode_set_framebuffer_state function in vrend_decode.c in virglrenderer before 926b9b3460a48f6454d8bbe9e44313d86a65447f, as used in Quick Emulator (QEMU), allows a local guest users to cause a denial of service (application crash) via the "nr_cbufs" argument.	2017-03-14	2.1	CVE-2017-5957 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM
virglrenderer_project -- virglrenderer	Heap-based buffer overflow in the vrend_create_vertex_elements_state function in vrend_renderer.c in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (out-of-bounds array access and crash) via the num_elements parameter.	2017-03-15	2.1	CVE-2017-5994 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM MLIST
virglrenderer_project -- virglrenderer	Stack-based buffer overflow in the parse_identifier function in tgsi_text.c in the TGSI auxiliary module in the Gallium driver in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (out-of-bounds array access and QEMU process crash) via vectors related to parsing properties.	2017-03-15	2.1	CVE-2017-6209 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM MLIST
virglrenderer_project -- virglrenderer	The vrend_decode_reset function in vrend_decode.c in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (NULL pointer dereference and QEMU process crash) by destroying context 0 (zero).	2017-03-15	2.1	CVE-2017-6210 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM MLIST
wordpress -- wordpress	In WordPress before 4.7.3, there is authenticated Cross-Site Scripting (XSS) via Media File Metadata. This is demonstrated by both (1) mishandling of the playlist shortcode in the wp_playlist_shortcode function in wp-includes/media.php and (2) mishandling of meta information in the renderTracks function in wp-includes/js/mediaelement/wp-	2017-03-11	3.5	CVE-2017-6814 MISC (link is external) BID (link is external) MISC MISC (link is external) MISC (link is external)

	playlist.js.			MISC
wordpress -- wordpress	In WordPress before 4.7.3 (wp-includes/embed.php), there is authenticated Cross-Site Scripting (XSS) in YouTube URL Embeds.	2017-03-11	3.5	CVE-2017-6817 BID (link is external) MISC MISC (link is external) MISC

- 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).