Vulnerability Summary for the Week of July 10, 2017

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

apache -- struts	The Struts 1 plugin in Apache Struts 2.3.x might allow remote code execution via a malicious field value passed in a raw message to the ActionMessage.	2017-07-10	7.5	CVE-2017-9791
				CONFIRM
				BID(link is external)
				SECTRACK(link is external)

cisco -- firesight_system_software	A vulnerability in the backup and restore functionality of Cisco FireSIGHT System Software could allow an authenticated, local attacker to execute arbitrary code on a targeted system. More Information: CSCvc91092. Known Affected Releases: 6.2.0 6.2.1.	2017-07-10	7.2	CVE-2017-6735
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

cisco -- prime_network	A vulnerability in the installation procedure for Cisco Prime Network Software could allow an authenticated, local attacker to elevate their privileges to root privileges. More Information: CSCvd47343. Known Affected Releases: 4.2(2.1)PP1 4.2(3.0)PP6 4.3(0.0)PP4 4.3(1.0)PP2. Known Fixed Releases: 4.3(2).	2017-07-10	7.2	CVE-2017-6732
				BID(link is external)
				CONFIRM(link is external)

dlink -- dir-615	On the D-Link DIR-615 before v20.12PTb04, once authenticated, this device identifies the user based on the IP address of his machine.	2017-07-07	7.5	CVE-2017-7405 MISC MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	By spoofing the IP address belonging to the victim's host, an attacker might be able to take over the administrative session without being prompted for authentication credentials. An attacker can get the victim's and router's IP addresses by simply sniffing the network traffic. Moreover, if the victim has web access enabled on his router and is accessing the web interface from a different network that is behind the NAT/Proxy, an attacker can sniff the network traffic to know the public IP address of the victim's router and take over his session as he won't be prompted for credentials.			
finecms_project -- finecms	FineCMS 2.1.0 allows remote attackers to execute arbitrary PHP code by using a URL Manager "Add Site" action to enter this code after a ', sequence in a domain name, as demonstrated by the ',phpinfo() input value.	2017-07-12	7.5	CVE-2017-11167 MISC(link is external)

foxitsoftware -- foxit_reader	Foxit Reader before 8.3.1 and PhantomPDF before 8.3.1 have an Arbitrary Write vulnerability, which allows remote attackers to execute arbitrary code via a crafted document.	2017-07-07	9.3	CVE-2017-10994
				BID(link is external)
				CONFIRM(link is external)

freedesktop -- systemd	systemd v233 and earlier fails to safely parse usernames starting with a numeric digit (e.g. "0day"), running the service in question with root privileges rather than the user intended.	2017-07-07	10.0	CVE-2017-1000082
				MLIST(link is external)
				BID(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

graphicsmagick -- graphicsmagick	GraphicsMagick 1.3.26 has double free vulnerabilities in the ReadOneJNGImage() function in coders/png.c.	2017-07-09	7.5	CVE-2017-11139
				CONFIRM(link is external)
				BID(link is external)

graphicsmagick -- graphicsmagick	The ReadJPEGImage function in coders/jpeg.c in GraphicsMagick 1.3.26 creates a pixel cache before a successful read of a scanline, which allows remote attackers to cause a denial of service (resource consumption) via crafted JPEG files.	2017-07-09	7.1	CVE-2017-11140
				CONFIRM(link is external)
				BID(link is external)

imagemagick -- imagemagick	The ReadMATImage function in coders\mat.c in ImageMagick 7.0.5-6 has a memory leak vulnerability that can cause memory exhaustion via a crafted MAT file, related to incorrect ordering of a SetImageExtent call.	2017-07-09	7.1	CVE-2017-11141
				BID(link is external)
				CONFIRM(link is external)

imagemagick -- imagemagick	The ReadXWDImage function in coders\xwd.c in ImageMagick 7.0.5-6 has a memory leak vulnerability that can cause memory exhaustion via a crafted length (number of color-map entries) field in the header of an XWD file.	2017-07-10	7.1	CVE-2017-11166 CONFIRM(link is external)
imagemagick -- imagemagick	The ReadDPXImage function in coders\dpx.c in ImageMagick 7.0.6-0 has a large loop vulnerability that can cause CPU exhaustion via a crafted DPX file, related to lack of an EOF check.	2017-07-12	7.8	CVE-2017-11188 CONFIRM(link is external)
irssi -- irssi	An issue was discovered in Irssi before 1.0.4. When receiving messages with invalid time stamps, Irssi	2017-07-07	7.5	CVE-2017-10965 CONFIRM(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	would try to dereference a NULL pointer.			
irssi -- irssi	An issue was discovered in Irssi before 1.0.4. While updating the internal nick list, Irssi could incorrectly use the GHashTable interface and free the nick while updating it. This would then result in use-after-free conditions on each access of the hash table.	2017-07-07	7.5	CVE-2017-10966 CONFIRM(link is external) CONFIRM
ismartalarm -- cube_one_firmware	On iSmartAlarm cube devices, there is authentication bypass leading to remote execution of commands (e.g., setting the alarm on/off), related to incorrect cryptography.	2017-07-11	7.5	CVE-2017-7728 MISC(link is external)
ismartalarm -- cube_one_firmware	iSmartAlarm cube devices allow Denial of Service. Sending a SYN flood on port 12345 will freeze the "cube" and it will stop responding.	2017-07-11	7.8	CVE-2017-7730 MISC(link is external)

kddi -- home_spot_cube_2_firmware	HOME SPOT CUBE2 firmware V101 and earlier allows an attacker to bypass authentication to load malicious firmware via WebUI.	2017-07-07	8.3	CVE-2017-2186
				JVN(link is external)
				BID(link is external)
				CONFIRM(link is external)

linux -- linux_kernel	The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact.	2017-07-11	10.0	CVE-2017-11176 CONFIRM CONFIRM(link is external)
mcafee -- advanced_threat_defense	Authentication Bypass vulnerability in the web interface in McAfee Advanced Threat Defense	2017-07-12	7.5	CVE-2017-4052 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(ATD) 3.10, 3.8, 3.6, 3.4 allows remote unauthenticated users / remote attackers to change or update any configuration settings, or gain administrator functionality via a crafted HTTP request parameter.			
mcafee -- advanced_threat_defense	Command Injection vulnerability in the web interface in McAfee Advanced Threat Defense (ATD) 3.10, 3.8, 3.6, 3.4 allows remote unauthenticated users / remote attackers to execute a command of their choice via a crafted HTTP request parameter.	2017-07-12	7.5	CVE-2017-4053 CONFIRM(link is external)

microsoft -- edge	Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8601,CVE-2017-8618, CVE-2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609.	2017-07-11	7.6	CVE-2017-8595
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- edge	Microsoft Edge in Microsoft Windows 10 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context	2017-07-11	7.6	CVE-2017-8596
				BID(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8598, CVE-2017-8610, CVE-2017-8595, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609.			

microsoft -- edge	Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8618, CVE-2017-8619, CVE-2017-8595, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609.	2017-07-11	7.6	CVE-2017-8598
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- edge	Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling	2017-07-11	7.6	CVE-2017-8601
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8618, CVE-2017-8619, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, CVE-2017-8598 and CVE-2017-8609.			

microsoft -- edge	Microsoft Edge in Microsoft Windows 10 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8598, CVE-2017-8618, CVE-2017-8619, CVE-2017-8595, CVE-2017-8601, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609.	2017-07-11	7.6	CVE-2017-8603
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- edge	Microsoft Edge in Microsoft Windows 10 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka	2017-07-11	7.6	CVE-2017-8604
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	"Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8618, CVE-2017-8619, CVE-2017-8601, CVE-2017-8610, CVE-2017-8603, CVE-2017-8598, CVE-2017-8601, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609.			

microsoft -- edge	Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8601, CVE-2017-8618, CVE-2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8598, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609.	2017-07-11	7.6	CVE-2017-8605
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- edge	Microsoft Internet Explorer in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Internet Explorer, aka "Scripting Engine Memory	2017-07-11	7.6	CVE-2017-8609
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Corruption Vulnerability". This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8618, CVE-2017-8619, CVE-2017-8595, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609.			

microsoft -- edge	Microsoft Edge in Microsoft Windows 10 1703 allows an attacker to execute arbitrary code in the context of the current user when the JavaScript engine fails to render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8598, CVE-2017-8596, CVE-2017-8595, CVE-2017-8618, CVE-2017-8619, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609.	2017-07-11	7.6	CVE-2017-8610
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- edge	Microsoft Edge in Windows 10 1703 Microsoft Edge allows a remote code execution vulnerability in the way affected Microsoft scripting engines render when handling objects in memory, aka "Microsoft Edge Remote Code Execution Vulnerability."	2017-07-11	7.6	CVE-2017-8617
				BID(link is external)
				CONFIRM(link is external)

microsoft -- edge	Microsoft Edge on Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows a remote code	2017-07-11	7.6	CVE-2017-8619 BID(link is external) SECTRACK(link

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution vulnerability in the way affected Microsoft scripting engines render when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, CVE-2017-8618, CVE-2017-9598 and CVE-2017-8609.			is external) CONFIRM(link is external)

microsoft -- excel	Microsoft Office allows a remote code execution vulnerability due to the way that it handles objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8501.	2017-07-11	9.3	CVE-2017-8502
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- internet_explorer	Microsoft browsers in Microsoft Windows 7, Windows Server 2008 and R2, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8598, CVE-2017-8596, CVE-2017-8618, CVE-	2017-07-11	7.6	CVE-2017-8606
				BID(link is external)
				SECTRACK(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8595, CVE-2017-8607, CVE-2017-8608, and CVE-2017-8609			

microsoft -- internet_explorer	Microsoft browsers in Microsoft Windows 7, Windows Server 2008 and R2, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling objects in memory in Microsoft browsers, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8598, CVE-2017-8596, CVE-2017-8618, CVE-2017-8619, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8595, CVE-2017-8606, CVE-2017-8608, and CVE-2017-8609	2017-07-11	7.6	CVE-2017-8607
				BID(link is external)
				SECTRACK(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- internet_explorer	Microsoft browsers in Microsoft Windows Server 2008 and R2, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user when the JavaScript engines fail to render when handling	2017-07-11	7.6	CVE-2017-8608
				BID(link is external)
				SECTRACK(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	objects in memory in Microsoft browsers, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8598, CVE-2017-8596, CVE-2017-8610, CVE-2017-8601, CVE-2017-8618, CVE-2017-8619, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8595, CVE-2017-8606, CVE-2017-8607, and CVE-2017-8609			

microsoft -- internet_explorer	Internet Explorer in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 Internet Explorer in the way affected Microsoft scripting engines render when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-8596, CVE-2017-8610, CVE-2017-8601, CVE-2017-8603, CVE-2017-8604, CVE-2017-8605, CVE-2017-8606, CVE-2017-8607, CVE-2017-8608, CVE-2017-8619, CVE-2017-9598 and CVE-2017-8609.	2017-07-11	7.6	CVE-2017-8618
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- office	Microsoft Office allows a remote code execution vulnerability due to the way that it handles objects in memory, aka "Microsoft Office Remote Code Execution Vulnerability".	2017-07-11	9.3	CVE-2017-8570
				BID(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This CVE ID is unique from CVE-2017-0243.			

microsoft -- office_online_server	Microsoft Office allows a remote code execution vulnerability due to the way that it handles objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-8502.	2017-07-11	9.3	CVE-2017-8501
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows_rt_8.1	Win32k in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability". This CVE ID is unique from CVE-2017-8577, CVE-2017-8580, CVE-2017-8581, and CVE-2017-8467.	2017-07-11	9.3	CVE-2017-8578
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows_rt_8.1	Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability due to the way that Windows Search handles objects in memory, aka "Windows Search Remote Code Execution Vulnerability".	2017-07-11	10.0	CVE-2017-8589
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

nfsen -- nfsen	NfSen before 1.3.8 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the customfmt parameter (aka the "Custom output format" field).	2017-07-10	9.0	CVE-2017-7175
				CONFIRM(link is external)
				EXPLOIT-DB(link is external)

pcre -- pcre	In PCRE 8.41, the OP_KETRMAX feature in the match function in pcre_exec.c allows stack exhaustion (uncontrolled recursion) when processing a crafted regular expression.	2017-07-10	7.8	CVE-2017-11164 MISC(link is external)
php -- php	In PHP before 5.6.31, 7.x before 7.0.17, and 7.1.x before 7.1.3, remote attackers could cause a CPU consumption denial of service attack by injecting long form variables, related to main/php_variables.c.	2017-07-10	7.8	CVE-2017-11142 CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)

schneider_electric -- wonderware_archestra_logger	A Stack-Based Buffer Overflow issue was discovered in Schneider Electric Wonderware ArchestrA Logger, versions 2017.426.2307.1 and prior. The stack-based buffer overflow vulnerability has been identified, which may allow a remote attacker to execute arbitrary code in the context of a highly privileged account.	2017-07-07	10.0	CVE-2017-9629
				MISC(link is external)
				BID(link is external)
				SECTRACK(link is external)
				MISC

sqlite -- sqlite	The getNodeSize function in ext/rtree/rtree.c in SQLite through 3.19.3, as used in GDAL and other products,	2017-07-07	7.5	CVE-2017-10989 MISC(link is external) BID(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mishandles undersized RTree blobs in a crafted database, leading to a heap-based buffer over-read or possibly unspecified other impact.			external) MISC MISC(link is external) MISC MISC
toshiba -- hem-gw26a_firmware	Toshiba Home gateway HEM-GW16A firmware HEM-GW16A-FW-V1.2.0 and earlier, Toshiba Home gateway HEM-GW26A firmware HEM-GW26A-FW-V1.2.0 and earlier may allow remote attackers to access a non-documented developer screen to perform operations on device with administrative privileges.	2017-07-07	7.5	CVE-2017-2234 JVN(link is external)
toshiba -- hem-gw26a_firmware	Toshiba Home gateway HEM-GW16A firmware HEM-GW16A-FW-V1.2.0 and earlier, Toshiba Home gateway HEM-GW26A firmware HEM-GW26A-FW-V1.2.0 and earlier uses hard-coded credentials, which may allow attackers to perform operations on device with administrative privileges.	2017-07-07	7.5	CVE-2017-2236 JVN(link is external)
toshiba -- hem-gw26a_firmware	Toshiba Home gateway HEM-GW16A firmware HEM-GW16A-FW-V1.2.0 and earlier. Toshiba Home gateway HEM-GW26A firmware HEM-GW26A-FW-V1.2.0 and earlier allows an attacker to execute arbitrary OS commands via unspecified vectors.	2017-07-07	10.0	CVE-2017-2237 JVN(link is external)
xar_project -- xar	libxar.so in xar 1.6.1 has a NULL pointer dereference in the xar_unserialize function in archive.c.	2017-07-09	7.5	CVE-2017-11124 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xar_project -- xar	libxar.so in xar 1.6.1 has a NULL pointer dereference in the xar_get_path function in util.c.	2017-07-09	7.5	CVE-2017-11125 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

apple -- quicktime	Untrusted search path vulnerability in Installer of QuickTime for Windows allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-07-07	6.8	CVE-2017-2218
				JVN(link is external)
				MISC(link is external)

brother_industries -- mfc-j960dwn_firmware	Cross-site request forgery (CSRF) vulnerability in MFC-J960DWN firmware ver.D and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2017-07-07	6.8	CVE-2017-2244
				JVN(link is external)
				CONFIRM(link is external)

charamin -- omp	Untrusted search path vulnerability in The installer of Charamin OMP Version 1.1.7.4 and earlier, Version 1.2.0.0 Beta and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-07-07	6.8	CVE-2017-2227 JVN(link is external)

cisco -- asr_5000_series	A vulnerability in the Border Gateway Protocol (BGP) processing functionality of the Cisco StarOS operating system for Cisco ASR 5000 Series Routers and Cisco Virtualized Packet Core (VPC) Software could allow an	2017-07-10	5.0	CVE-2017-6729
				SECTRACK(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthenticated, remote attacker to cause the BGP process on an affected system to reload, resulting in a denial of service (DoS) condition. This vulnerability affects the following products if they are running the Cisco StarOS operating system and BGP is enabled for the system: Cisco ASR 5000 Series Routers and Cisco Virtualized Packet Core Software. More Information: CSCvc44968. Known Affected Releases: 16.4.1 19.1.0 21.1.0 21.1.M0.65824. Known Fixed Releases: 21.3.A0.65902 21.2.A0.65905 21.1.b0.66164 21.1.V0.66014 21.1.R0.65898 21.1.M0.65894 21.1.0.66030 21.1.0.			

cisco -- identity_services_engine	A vulnerability in the web-based application interface of the Cisco Identity Services Engine (ISE) portal could allow an unauthenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web interface of an affected system. More Information: CSCvd87482. Known Affected Releases: 2.1(102.101) 2.2(0.283) 2.3(0.151).	2017-07-10	4.3	CVE-2017-6733
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

cisco -- ios_xr	A vulnerability in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to execute arbitrary code at the root privilege level on an affected system, because of Incorrect Permissions. More	2017-07-10	6.9	CVE-2017-6728
				BID(link is external)
				SECTRACK(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Information: CSCvb99389. Known Affected Releases: 6.2.1.BASE. Known Fixed Releases: 6.3.1.15i.BASE 6.2.3.1i.BASE 6.2.2.15i.BASE 6.1.4.10i.BASE.			CONFIRM(link is external)

cisco -- ios_xr	A vulnerability in Multicast Source Discovery Protocol (MSDP) ingress packet processing for Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause the MSDP session to be unexpectedly reset, causing a short denial of service (DoS) condition. The MSDP session will restart within a few seconds. More Information: CSCvd94828. Known Affected Releases: 4.3.2.MCAST 6.0.2.BASE. Known Fixed Releases: 6.3.1.19i.MCAST 6.2.3.1i.MCAST 6.2.2.17i.MCAST 6.1.4.12i.MCAST.	2017-07-10	5.0	CVE-2017-6731
				SECTRACK(link is external)
				CONFIRM(link is external)

cisco -- wide_area_application_services	A vulnerability in the Server Message Block (SMB) protocol of Cisco Wide Area Application Services (WAAS) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device due to a process restarting unexpectedly and creating Core Dump files. More Information: CSCvc63035. Known Affected Releases: 6.2(3a). Known Fixed	2017-07-10	5.0	CVE-2017-6727
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Releases: 6.3(0.167) 6.2(3c)5 6.2(3.22).			

cisco -- wide_area_application_services	A vulnerability in the web-based GUI of Cisco Wide Area Application Services (WAAS) Central Manager could allow an unauthenticated, remote attacker to retrieve completed reports from an affected system, aka Information Disclosure. This vulnerability affects the following products if they are running an affected release of Cisco Wide Area Application Services (WAAS) Software and are configured to use the Central Manager function: Cisco Virtual Wide Area Application Services (vWAAS), Cisco Wide Area Application Services (WAAS) Appliances, Cisco Wide Area Application Services (WAAS) Modules. Only Cisco WAAS products that are configured with the Central Manager role are affected by this vulnerability. More Information: CSCvd87574. Known Affected Releases: 4.4(7) 6.2(1) 6.2(3). Known Fixed Releases: 6.3(0.228) 6.3(0.226) 6.2(3d)8 5.5(7b)17.	2017-07-10	5.0	CVE-2017-6730
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

cybozu -- garoon	Cybozu Garoon 3.0.0 to 4.2.4 may allow an attacker to lock another user's file through a specially crafted page.	2017-07-07	5.8	CVE-2017-2144
				JVN(link is external)
				CONFIRM(link is external)

cybozu -- garoon	Session fixation vulnerability in Cybozu Garoon 4.0.0 to	2017-07-07	5.8	CVE-2017-2145

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

	4.2.4 allows remote attackers to perform arbitrary operations via unspecified vectors.			JVN(link is external)
				CONFIRM(link is external)

dfactory -- responsive_lightbox	Cross-site scripting vulnerability in Responsive Lightbox prior to version 1.7.2 allows an attacker to inject arbitrary web script or HTML via unspecified vectors.	2017-07-07	4.3	CVE-2017-2243
				JVN(link is external)
				BID(link is external)
				CONFIRM

dlink -- dir-615	On the D-Link DIR-615 before v20.12PTb04, if a victim logged in to the Router's Web Interface visits a malicious site from another Browser tab, the malicious site then can send requests to the victim's Router without knowing the credentials (CSRF). An attacker can host a page that sends a POST request to Form2File.htm that tries to upload Firmware to victim's Router. This causes the router to reboot/crash resulting in Denial of Service. An attacker may succeed in uploading malicious Firmware.	2017-07-07	6.8	CVE-2017-7404 MISC MISC(link is external)
dlink -- dir-615	The D-Link DIR-615 device before v20.12PTb04 doesn't use SSL for any of the authenticated pages. Also, it doesn't allow the user to generate his own SSL Certificate. An attacker can simply monitor network traffic to steal a user's credentials and/or credentials of users being added while sniffing the traffic.	2017-07-07	5.0	CVE-2017-7406 MISC MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
download_manager_project -- download_manager	Open redirect vulnerability in WordPress Download Manager prior to version 2.9.51 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2017-07-07	5.8	CVE-2017-2217 JVN(link is external) CONFIRM CONFIRM

etherpad -- etherpad	Directory traversal vulnerability in node/utils/Minify.js in Etherpad 1.1.1 through 1.5.2 allows remote attackers to read arbitrary files by leveraging replacement of backslashes with slashes in the path parameter of HTTP API requests.	2017-07-07	5.0	CVE-2015-3297
				MLIST(link is external)
				MLIST(link is external)
				BID(link is external)
				CONFIRM(link is external)

finecms_project -- finecms	FineCMS through 2017-07-11 has stored XSS in route=admin when modifying user information, and in route=register when registering a user account.	2017-07-11	4.3	CVE-2017-11179 MISC(link is external)
finecms_project -- finecms	FineCMS through 2017-07-11 has stored XSS in the logging functionality, as demonstrated by an XSS payload in (1) the User-Agent header of an HTTP request or (2) the username entered on the login screen.	2017-07-11	4.3	CVE-2017-11180 MISC(link is external)
finecms_project -- finecms	Cross-site scripting (XSS) vulnerability in /application/lib/ajax/get_image.php in FineCMS through 2017-07-12 allows remote attackers to inject arbitrary web script or HTML via the folder, id, or name parameter.	2017-07-12	4.3	CVE-2017-11198 MISC(link is external)
finecms_project -- finecms	SQL Injection exists in FineCMS through 2017-07-12	2017-07-12	6.5	CVE-2017-11200

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	via the application/core/controller/excludes.php visitor_ip parameter.			MISC(link is external)
finecms_project -- finecms	FineCMS through 2017-07-12 allows XSS in visitors.php because JavaScript in visited URLs is not restricted either during logging or during the reading of logs, a different vulnerability than CVE-2017-11180.	2017-07-12	4.3	CVE-2017-11202 MISC(link is external)
fossies -- catdoc	The ole_init function in ole.c in catdoc 0.95 allows remote attackers to cause a denial of service (heap-based buffer underflow and application crash) or possibly have unspecified other impact via a crafted file, i.e., data is written to memory addresses before the beginning of the tmpBuf buffer.	2017-07-08	6.8	CVE-2017-11110 MISC(link is external)
gnu -- ncurses	In ncurses 6.0, there is an attempted 0xffffffffffffffff access in the append_acs function of tinfo/parse_entry.c. It could lead to a remote denial of service attack if the terminfo library code is used to process untrusted terminfo data.	2017-07-08	5.0	CVE-2017-11112 MISC(link is external)
gnu -- ncurses	In ncurses 6.0, there is a NULL Pointer Dereference in the _nc_parse_entry function of tinfo/parse_entry.c. It could lead to a remote denial of service attack if the terminfo library code is used to process untrusted terminfo data.	2017-07-08	5.0	CVE-2017-11113 MISC(link is external)
google -- android	Race condition in the bindBackupAgent method in the ActivityManagerService in Android 4.4.4 allows local	2017-07-07	6.9	CVE-2014-7953 FULLDISC BUGTRAQ

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

	users with adb shell access to execute arbitrary code or any valid package as system by running "pm install" with the target apk, and simultaneously running a crafted script to process logcat's output looking for a dexopt line, which once found should execute bindBackupAgent with the uid member of the ApplicationInfo parameter set to 1000.			(link is external)
				BID(link is external)
				CONFIRM(link is external)

graphicsmagick -- graphicsmagick	The ReadOneJNGImage function in coders/png.c in GraphicsMagick 1.3.26 allows remote attackers to cause a denial of service (application crash) during JNG reading via a zero-length color_image data structure.	2017-07-07	5.0	CVE-2017-11102
				CONFIRM(link is external)
				CONFIRM(link is external)
				BID(link is external)

ibm -- infosphere_information_server	IBM InfoSphere Information Server 9.1, 11.3, and 11.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 125916.	2017-07-12	4.3	CVE-2017-1321
				CONFIRM(link is external)
				MISC(link is external)

ibm -- websphere_mq	IBM WebSphere MQ 9.0.1 and 9.0.2 Java/JMS application can incorrectly transmit user credentials in plain text. IBM X-Force ID: 126245.	2017-07-10	4.3	CVE-2017-1337
				CONFIRM(link is external)
				BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC(link is external)

imagemagick -- imagemagick	The mng_get_long function in coders/png.c in ImageMagick 7.0.6-0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted MNG image.	2017-07-07	4.3	CVE-2017-10995
				BID(link is external)
				CONFIRM(link is external)

iodata -- ts-wlce_camera_firmware	Cross-site request forgery (CSRF) vulnerability in TS-WPTCAM, TS-PTCAM, TS-PTCAM/POE, TS-WLC2, TS-WLCE, TS-WRLC firmware version 1.19 and earlier and TS-WPTCAM2 firmware version 1.01 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2017-07-07	6.8	CVE-2017-2223
				MISC(link is external)
				BID(link is external)
				JVN(link is external)

ismartalarm -- cube_one_firmware	iSmartAlarm cube devices have an SSL Certificate Validation Vulnerability.	2017-07-11	5.0	CVE-2017-7726 MISC(link is external)
ismartalarm -- cube_one_firmware	On iSmartAlarm cube devices, there is Incorrect Access Control because a "new key" is transmitted in cleartext.	2017-07-11	5.0	CVE-2017-7729 MISC(link is external)

kddi -- home_spot_cube_2_firmware	HOME SPOT CUBE2 firmware V101 and earlier allows authenticated attackers to execute arbitrary OS commands via Clock Settings.	2017-07-07	5.2	CVE-2017-2183
				JVN(link is external)
				BID(link is external)
				CONFIRM(link is external)

kddi -- home_spot_cube_2_firmware	Buffer overflow in HOME SPOT CUBE2 firmware V101 and earlier allows an attacker	2017-07-07	5.8	CVE-2017-2184 JVN(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

	to execute arbitrary code via WebUI.			BID(link is external)
				CONFIRM(link is external)

kddi -- home_spot_cube_2_firmware	HOME SPOT CUBE2 firmware V101 and earlier allows authenticated attackers to execute arbitrary OS commands via WebUI.	2017-07-07	5.2	CVE-2017-2185
				JVN(link is external)
				BID(link is external)
				CONFIRM(link is external)

knot-dns -- knot_dns	Knot DNS before 2.4.5 and 2.5.x before 2.5.2 contains a flaw within the TSIG protocol implementation that would allow an attacker with a valid key name and algorithm to bypass TSIG authentication if no additional ACL restrictions are set, because of an improper TSIG validity period check.	2017-07-08	4.3	CVE-2017-11104 MISC(link is external) MISC MISC(link is external)
marp_project -- marp	Marp versions v0.0.10 and earlier may allow an attacker to access local resources and files using JavaScript.	2017-07-07	6.8	CVE-2017-2239 JVN(link is external)
mcafee -- advanced_threat_defense	Command Injection vulnerability in the web interface in McAfee Advanced Threat Defense (ATD) 3.10, 3.8, 3.6, 3.4 allows remote authenticated users to execute a command of their choice via a crafted HTTP request parameter.	2017-07-12	6.5	CVE-2017-4054 CONFIRM(link is external)
mcafee -- advanced_threat_defense	Exploitation of Authentication vulnerability in the web interface in McAfee Advanced Threat Defense (ATD) 3.10, 3.8, 3.6, 3.4 allows remote	2017-07-12	5.0	CVE-2017-4055 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthenticated users / remote attackers to bypass ATD detection via loose enforcement of authentication and authorization.			
mcafee -- advanced_threat_defense	Privilege Escalation vulnerability in the web interface in McAfee Advanced Threat Defense (ATD) 3.10, 3.8, 3.6, 3.4 allows remote authenticated users to gain elevated privileges via the GUI or GUI terminal commands.	2017-07-12	6.5	CVE-2017-4057 CONFIRM(link is external)

mext -- ebidsettingchecker	Untrusted search path vulnerability in EbidSettingChecker.exe (version 1.0.0.0) allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-07-07	6.8	CVE-2017-2225
				JVN(link is external)
				MISC(link is external)

microsoft -- edge	Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to trick a user into loading a page with malicious content when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents, aka "Microsoft Edge Security Feature Bypass Vulnerability".	2017-07-11	4.3	CVE-2017-8599
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- edge	Microsoft Edge on Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows remote attackers to spoof web content via a crafted web site, aka "Microsoft Edge Spoofing Vulnerability."	2017-07-11	4.3	CVE-2017-8611
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

microsoft -- exchange_server	Microsoft Exchange Server 2010 SP3, Exchange Server 2013 SP3, Exchange Server 2013 CU16, and Exchange Server 2016 CU5 allows an elevation of privilege vulnerability due to the way that Exchange Outlook Web Access (OWA) handles web requests, aka "Microsoft Exchange Cross-Site Scripting Vulnerability". This CVE ID is unique from CVE-2017-8560.	2017-07-11	4.3	CVE-2017-8559
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- exchange_server	Microsoft Exchange Server 2010 SP3, Exchange Server 2013 SP3, Exchange Server 2013 CU16, and Exchange Server 2016 CU5 allows an elevation of privilege vulnerability due to the way that Exchange Outlook Web Access (OWA) handles web requests, aka "Microsoft Exchange Cross-Site Scripting Vulnerability". This CVE ID is unique from CVE-2017-8559.	2017-07-11	4.3	CVE-2017-8560
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- internet_explorer	Microsoft browsers on Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow a spoofing vulnerability in the way they parse HTTP content, aka "Microsoft Browser Spoofing Vulnerability."	2017-07-11	4.3	CVE-2017-8602
				BID(link is external)
				SECTRACK(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- sharepoint_server	Microsoft SharePoint Server allows an elevation of privilege vulnerability due to	2017-07-11	6.5	CVE-2017-8569 BID(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

	the way that it sanitizes a specially crafted web request to an affected SharePoint server, aka "SharePoint Server XSS Vulnerability".			external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows_10	Microsoft Windows 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to Windows Input Method Editor (IME) improperly handling parameters in a method of a DCOM class, aka "Windows IME Elevation of Privilege Vulnerability".	2017-07-11	4.4	CVE-2017-8566
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows_rt_8.1	Windows kernel in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to the way it handles objects in memory, aka "Windows Kernel Elevation of Privilege Vulnerability".	2017-07-11	6.9	CVE-2017-8561
				BID(link is external)
				CONFIRM(link is external)

microsoft -- windows_rt_8.1	Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to Kerberos falling back to NT LAN Manager (NTLM) Authentication Protocol as the default authentication protocol,	2017-07-11	5.1	CVE-2017-8563
				BID(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	aka "Windows Elevation of Privilege Vulnerability".			

microsoft -- windows_rt_8.1	Win32k in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability". This CVE ID is unique from CVE-2017-8578, CVE-2017-8580, CVE-2017-8581, and CVE-2017-8467.	2017-07-11	6.9	CVE-2017-8577
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows_rt_8.1	Win32k in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability". This CVE ID is unique from CVE-2017-8577, CVE-2017-8578, CVE-2017-8581, and CVE-2017-8467.	2017-07-11	6.2	CVE-2017-8580
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows_rt_8.1	Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an elevation of	2017-07-11	4.6	CVE-2017-8590
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privilege vulnerability due to the way that the Windows Common Log File System (CLFS) driver handles objects in memory, aka "Windows CLFS Elevation of Privilege Vulnerability".			link is external)
mpg123 -- mpg123	The III_i_stereo function in libmpg123/layer3.c in mpg123 through 1.25.1 allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted audio file that is mishandled in the code for the "block_type != 2" case, a similar issue to CVE-2017-9870.	2017-07-09	4.3	CVE-2017-11126 MISC(link is external) MISC

national_tax_agency -- e-tax	Untrusted search path vulnerability in Setup file of advance preparation for e-Tax software (WEB version) (1.17.1) and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-07-07	6.8	CVE-2017-2226
				JVN(link is external)
				BID(link is external)

nilim -- road_construction_completion_diagram_check_program	Untrusted search path vulnerability in Douro Kouji Kanseizutou Check Program Ver3.1 (cdrw_checker_3.1.0.lzh) and earlier allows remote attackers to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-07-07	6.8	CVE-2017-2230
				JVN(link is external)
				MISC(link is external)
				MISC(link is external)

nitro -- nitro_pro	Nitro Pro 11.0.3 and earlier allows remote attackers to cause a denial of service (application crash) via a crafted PCX file.	2017-07-07	4.3	CVE-2017-7950
				BID(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
php -- php	In PHP before 5.6.28 and 7.x before 7.0.13, incorrect handling of various URI components in the URL parser could be used by attackers to bypass hostname-specific URL checks, as demonstrated by evil.example.com:80#@good.example.com/ and evil.example.com:80?@good.example.com/ inputs to the parse_url function (implemented in the php_url_parse_ex function in ext/standard/url.c).	2017-07-10	5.0	CVE-2016-10397 CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)
php -- php	In PHP before 5.6.31, an invalid free in the WDDX deserialization of boolean parameters could be used by attackers able to inject XML for deserialization to crash the PHP interpreter, related to an invalid free for an empty boolean element in ext/wddx/wddx.c.	2017-07-10	5.0	CVE-2017-11143 CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)
php -- php	In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, the openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function, which could lead to a crash of the PHP interpreter, related to an interpretation conflict for a negative number in ext/openssl/openssl.c, and an	2017-07-10	5.0	CVE-2017-11144 CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	OpenSSL documentation omission.			CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)
php -- php	In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, lack of a bounds check in the date extension's timelib_meridian parsing code could be used by attackers able to supply date strings to leak information from the interpreter, related to an ext/date/lib/parse_date.c out-of-bounds read affecting the php_parse_date function.	2017-07-10	5.0	CVE-2017-11145 CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)
php -- php	In PHP before 5.6.30 and 7.x before 7.0.15, the PHAR archive handler could be used by attackers supplying malicious archive files to crash the PHP interpreter or potentially disclose information due to a buffer over-read in the phar_parse_pharfile function in ext/phar/phar.c.	2017-07-10	6.4	CVE-2017-11147 CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				external) CONFIRM(link is external)
phpldapadmin -- phpldapadmin	phpLDAPadmin through 1.2.3 has XSS in htdocs/entry_chooser.php via the form, element, rdn, or container parameter.	2017-07-08	4.3	CVE-2017-11107 MISC(link is external) MISC(link is external)

schneider_electric -- wonderware_archestra_logger	An Uncontrolled Resource Consumption issue was discovered in Schneider Electric Wonderware ArchestrA Logger, versions 2017.426.2307.1 and prior. The uncontrolled resource consumption vulnerability could allow an attacker to exhaust the memory resources of the machine, causing a denial of service.	2017-07-07	5.0	CVE-2017-9627
				MISC(link is external)
				BID(link is external)
				SECTRACK(link is external)
				MISC

schneider_electric -- wonderware_archestra_logger	A Null Pointer Dereference issue was discovered in Schneider Electric Wonderware ArchestrA Logger, versions 2017.426.2307.1 and prior. The null pointer dereference vulnerability could allow an attacker to crash the logger process, causing a denial of service for logging and log-viewing (applications that use the Wonderware ArchestrA Logger continue to run when the Wonderware ArchestrA Logger service is unavailable).	2017-07-07	5.0	CVE-2017-9631
				MISC(link is external)
				BID(link is external)
				SECTRACK(link is external)
				MISC

shortcodes_ultimate_project -- shortcodes_ultimate	Directory traversal vulnerability in Shortcodes Ultimate prior to version 4.10.0 allows remote attackers	2017-07-07	4.0	CVE-2017-2245 BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to read arbitrary files via unspecified vectors.			JVN(link is external) CONFIRM CONFIRM
swftools -- swftools	When SWFTools 0.9.2 processes a crafted file in swfcombine, it can lead to a NULL Pointer Dereference in the swf_DeleteFilter() function in lib/modules/swffilter.c.	2017-07-07	6.8	CVE-2017-11096 MISC(link is external)
swftools -- swftools	When SWFTools 0.9.2 processes a crafted file in swfc, it can lead to a NULL Pointer Dereference in the dict_lookup() function in lib/q.c.	2017-07-07	6.8	CVE-2017-11097 MISC(link is external)
swftools -- swftools	When SWFTools 0.9.2 processes a crafted file in png2swf, it can lead to a Segmentation Violation in the png_load() function in lib/png.c.	2017-07-07	6.8	CVE-2017-11098 MISC(link is external)
swftools -- swftools	When SWFTools 0.9.2 processes a crafted file in wav2swf, it can lead to a Segmentation Violation in the wav_convert2mono() function in lib/wav.c.	2017-07-07	6.8	CVE-2017-11099 MISC(link is external)
swftools -- swftools	When SWFTools 0.9.2 processes a crafted file in swfextract, it can lead to a NULL Pointer Dereference in the swf_FoldSprite() function in lib/rxfswf.c.	2017-07-07	6.8	CVE-2017-11100 MISC(link is external)
swftools -- swftools	When SWFTools 0.9.2 processes a crafted file in swfcombine, it can lead to a NULL Pointer Dereference in the swf_Relocate() function in lib/modules/swftools.c.	2017-07-07	6.8	CVE-2017-11101 MISC(link is external)
tcpdump -- tcpdump	tcpdump 4.9.0 allows remote attackers to cause a denial of	2017-07-08	5.0	CVE-2017-11108

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	service (heap-based buffer over-read and application crash) via crafted packet data. The crash occurs in the EXTRACT_16BITS function, called from the stp_print function for the Spanning Tree Protocol.			MISC(link is external)
toshiba -- hem-gw26a_firmware	Toshiba Home gateway HEM-GW16A firmware HEM-GW16A-FW-V1.2.0 and earlier. Toshiba Home gateway HEM-GW26A firmware HEM-GW26A-FW-V1.2.0 and earlier allows an attacker to bypass access restriction to change the administrator account password via unspecified vectors.	2017-07-07	5.0	CVE-2017-2235 JVN(link is external)
toshiba -- hem-gw26a_firmware	Cross-site request forgery (CSRF) vulnerability in Toshiba Home gateway HEM-GW16A firmware HEM-GW16A-FW-V1.2.0 and earlier and Toshiba Home gateway HEM-GW26A firmware HEM-GW26A-FW-V1.2.0 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2017-07-07	6.8	CVE-2017-2238 JVN(link is external)

vim -- vim	Vim 8.0 allows attackers to cause a denial of service (invalid free) or possibly have unspecified other impact via a crafted source (aka -S) file. NOTE: there might be a limited number of scenarios in which this has security relevance.	2017-07-08	6.8	CVE-2017-11109
				MISC(link is external)
				MISC.(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
web-dorado -- event_calendar_wd	Cross-site scripting vulnerability in Event Calendar WD prior to version 1.0.94 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-07-07	4.3	CVE-2017-2224 BID(link is external) JVN(link is external) CONFIRM CONFIRM
wp-members_project -- wp-members	Cross-site scripting vulnerability in WP-Members prior to version 3.1.8 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-07-07	4.3	CVE-2017-2222 JVN(link is external) CONFIRM CONFIRM
wp-statistics -- wp_statistics	The WP Statistics plugin through 12.0.9 for WordPress has XSS in the rangestart and rangeend parameters on the wps_referrers_page page.	2017-07-07	4.3	CVE-2017-10991 MISC(link is external)
wpdownloadmanager -- download_manager	Cross-site scripting vulnerability in WordPress Download Manager prior to version 2.9.50 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-07-07	4.3	CVE-2017-2216 JVN(link is external) CONFIRM CONFIRM

yaws -- yaws	Yaws 1.91 allows Unauthenticated Remote File Disclosure via HTTP Directory Traversal with /%5C../ to port 8080. NOTE: this CVE is only about use of an initial /%5C sequence to defeat traversal protection mechanisms; the initial /%5C sequence was apparently not discussed in earlier research on this product.	2017-07-07	5.0	CVE-2017-10974
				MISC
				BID(link is external)
				EXPLOIT-DB(link is external)

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cacti -- cacti	Cross-site scripting (XSS) vulnerability in aggregate_graphs.php in Cacti 1.1.12 allows remote authenticated users to inject arbitrary web script or HTML via specially crafted HTTP Referer headers, related to the $cancel_url variable.	2017-07-10	3.5	CVE-2017-11163 CONFIRM(link is external)

cisco -- identity_services_engine	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web interface of an affected device, related to the Guest Portal. More Information: CSCvd74794. Known Affected Releases: 1.3(0.909) 2.1(0.800).	2017-07-10	3.5	CVE-2017-6734
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

cisco -- prime_network	A vulnerability in the CLI of the Cisco Prime Network Gateway could allow an authenticated, local attacker to retrieve system process information, which could lead to the disclosure of confidential information. More Information: CSCvd59341. Known Affected Releases: 4.2(1.0)P1.	2017-07-10	2.1	CVE-2017-6726
				BID(link is external)
				CONFIRM(link is external)

cybozu -- garoon	Cross-site scripting vulnerability in Cybozu Garoon 3.0.0 to 4.2.4 allows remote attackers to inject arbitrary web script or HTML via application menu.	2017-07-07	3.5	CVE-2017-2146
				JVN(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fairsketch -- rise_ultimate_project_manager	In Rise Ultimate Project Manager v1.8, XSS vulnerabilities were found in the Messaging section. Subject and Message fields are vulnerable.	2017-07-11	3.5	CVE-2017-11181 MISC(link is external)
fairsketch -- rise_ultimate_project_manager	In Rise Ultimate Project Manager v1.8, XSS vulnerabilities were found in the My Profile section. All input fields are vulnerable.	2017-07-11	3.5	CVE-2017-11182 MISC(link is external)
finecms_project -- finecms	application/core/controller/images.php in FineCMS through 2017-07-12 allows remote authenticated admins to conduct XSS attacks by uploading an image via a route=images action.	2017-07-12	3.5	CVE-2017-11201 MISC(link is external)

google -- android	Directory traversal vulnerability in the doSendObjectInfo method in frameworks/av/media/mtp/MtpServer.cpp in Android 4.4.4 allows physically proximate attackers with a direct connection to the target Android device to upload files outside of the sdcard via a .. (dot dot) in a name parameter of an MTP request.	2017-07-07	2.1	CVE-2014-7954
				MISC(link is external)
				FULLDISC
				BUGTRAQ(link is external)
				BID(link is external)

ibm -- websphere_mq	IBM WebSphere MQ 9.0.1 and 9.0.2 could allow a local user with ability to run or enable trace, to obtain sensitive information from WebSphere Application Server traces including user credentials. IBM X-Force ID: 125145.	2017-07-10	1.9	CVE-2017-1284
				CONFIRM(link is external)
				BID(link is external)
				MISC(link is external)

microsoft -- windows_rt_8.1	Win32k in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability". This CVE	2017-07-11	3.7	CVE-2017-8581
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ID is unique from CVE-2017-8578, CVE-2017-8580, CVE-2017-8577, and CVE-2017-8467.			

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- httpd	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.	2017-07-13	not yet calculated	CVE-2017-9788 CONFIRM CONFIRM MLIST
apache -- httpd	When under stress, closing many connections, the HTTP/2 handling code in Apache httpd 2.4.26 would sometimes access memory after it has been freed, resulting in potentially erratic behaviour.	2017-07-13	not yet calculated	CVE-2017-9789 CONFIRM MLIST
apache -- impala	During a routine security analysis, it was found that one of the ports in Apache Impala (incubating) 2.7.0 to 2.8.0 sent data in plaintext even when	2017-07-10	not yet calculated	CVE-2017-5652 MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the cluster was configured to use TLS. The port in question was used by the StatestoreSubscriber class which did not use the appropriate secure Thrift transport when TLS was turned on. It was therefore possible for an adversary, with access to the network, to eavesdrop on the packets going to and coming from that port and view the data in plaintext.			
apache -- impala	It was noticed that a malicious process impersonating an Impala daemon in Apache Impala (incubating) 2.7.0 to 2.8.0 could cause Impala daemons to skip authentication checks when Kerberos is enabled (but TLS is not). If the malicious server responds with 'COMPLETE' before the SASL handshake has completed, the client will consider the handshake as completed even though no exchange of credentials has happened.	2017-07-10	not yet calculated	CVE-2017-5640 BID(link is external) MLIST
apache -- solr	Apache Solr uses a PKI based mechanism to secure inter-node communication when security is enabled. It is possible to create a specially crafted node name that does not exist as part of the cluster and point it to a malicious node. This can trick the nodes in cluster to believe that the malicious node is a member of the cluster. So, if Solr users have enabled BasicAuth authentication mechanism	2017-07-07	not yet calculated	CVE-2017-7660 MLIST BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	using the BasicAuthPlugin or if the user has implemented a custom Authentication plugin, which does not implement either "HttpClientInterceptorPlugin" or "HttpClientBuilderPlugin", his/her servers are vulnerable to this attack. Users who only use SSL without basic authentication or those who use Kerberos are not affected.			
apache -- spark	In Apache Spark before 2.2.0, it is possible for an attacker to take advantage of a user's trust in the server to trick them into visiting a link that points to a shared Spark cluster and submits data including MHTML to the Spark master, or history server. This data, which could contain a script, would then be reflected back to the user and could be evaluated and executed by MS Windows-based clients. It is not an attack on Spark itself, but on the user, who may then execute the script inadvertently when viewing elements of the Spark web UIs.	2017-07-12	not yet calculated	CVE-2017-7678 MLIST(link is external)
apache -- struts	If an application allows enter an URL in a form field and built-in URLValidator is used, it is possible to prepare a special URL which will be used to overload server process when performing validation of the URL. Solution is to upgrade to Apache Struts version 2.5.12.	2017-07-13	not yet calculated	CVE-2017-7672 CONFIRM MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- struts	When using a Spring AOP functionality to secure Struts actions it is possible to perform a DoS attack when user was properly authenticated. Solution is to upgrade to Apache Struts version 2.5.12 or 2.3.33.	2017-07-13	not yet calculated	CVE-2017-9787 CONFIRM MLIST
apache -- traffic_router	The Traffic Router component of the incubating Apache Traffic Control project is vulnerable to a Slowloris style Denial of Service attack. TCP connections made on the configured DNS port will remain in the ESTABLISHED state until the client explicitly closes the connection or Traffic Router is restarted. If connections remain in the ESTABLISHED state indefinitely and accumulate in number to match the size of the thread pool dedicated to processing DNS requests, the thread pool becomes exhausted. Once the thread pool is exhausted, Traffic Router is unable to service any DNS request, regardless of transport protocol.	2017-07-10	not yet calculated	CVE-2017-7670 MLIST
avg -- antivirus	AVG AntiVirus for MacOS with scan engine before 4668 might allow remote attackers to bypass malware detection by leveraging failure to scan inside disk image (aka DMG) files.	2017-07-12	not yet calculated	CVE-2017-9977 MISC(link is external)
canonical -- ubuntu	ubuntu-image 1.0 before 2017-07-07, when invoked as non-root, creates files in the resulting image with the uid of the invoking user. When the resulting image is booted, a	2017-07-11	not yet calculated	CVE-2017-10600 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	local attacker with the same uid as the image creator has unintended access to cloud-init and snapd directories.			
cloud_foundry -- cloud_foundry	In Cloud Foundry cf-release versions prior to v264; UAA release all versions of UAA v2.x.x, 3.6.x versions prior to v3.6.13, 3.9.x versions prior to v3.9.15, 3.20.x versions prior to v3.20.0, and other versions prior to v4.4.0; and UAA bosh release (uaa-release) 13.x versions prior to v13.17, 24.x versions prior to v24.12. 30.x versions prior to 30.5, and other versions prior to v41, zone administrators are allowed to escalate their privileges when mapping permissions for an external provider.	2017-07-10	not yet calculated	CVE-2017-8032 CONFIRM
emc -- data_protection_advisor	EMC Data Protection Advisor prior to 6.4 contains a path traversal vulnerability. A remote authenticated high privileged user may potentially exploit this vulnerability to access unauthorized information from the underlying OS server by supplying specially crafted strings in input parameters of the application.	2017-07-09	not yet calculated	CVE-2017-8003 CONFIRM BID(link is external) SECTRACK (link is external)
emc -- data_protection_advisor	EMC Data Protection Advisor prior to 6.4 contains multiple blind SQL injection vulnerabilities. A remote authenticated attacker may potentially exploit these vulnerabilities to gain information about the application by causing	2017-07-09	not yet calculated	CVE-2017-8002 CONFIRM BID(link is external) SECTRACK (link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution of arbitrary SQL commands.			
emc -- esrs_policy_manager	EMC ESRS Policy Manager prior to 6.8 contains an undocumented account (OpenDS admin) with a default password. A remote attacker with the knowledge of the default password may login to the system and gain administrator privileges to the local LDAP directory server.	2017-07-09	not yet calculated	CVE-2017-4976 CONFIRM SECTRACK (link is external)
finecms -- finecms	In FineCMS through 2017-07-11, application/core/controller/style.php allows remote attackers to write to arbitrary files via the contents and filename parameters in a route=style action. For example, this can be used to overwrite a .php file because the file extension is not checked.	2017-07-11	not yet calculated	CVE-2017-11178 MISC(link is external)
gnome_project -- gnome	Bad reference counting in the context of accept_ice_connection() in gsm-xsmp-server.c in old versions of gnome-session up until version 2.29.92 allows a local attacker to establish ICE connections to gnome-session with invalid authentication data (an invalid magic cookie). Each failed authentication attempt will leak a file descriptor in gnome-session. When the maximum number of file descriptors is exhausted in the gnome-session process, it will enter an infinite loop trying to communicate without success, consuming 100% of the CPU. The graphical session associated with the	2017-07-11	not yet calculated	CVE-2017-11171 CONFIRM(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	gnome-session process will stop working correctly, because communication with gnome-session is no longer possible.			
google -- android	An elevation of privilege vulnerability in the NVIDIA sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A-34373711. References: N-CVE-2017-6249.	2017-07-13	not yet calculated	CVE-2017-6249 CONFIRM(link is external)

google -- android	An elevation of privilege vulnerability in the NVIDIA Libnvparser component due to a memcpy into a fixed sized buffer with a user-controlled size could lead to a memory corruption and possible remote code execution. This issue is rated as High. Product: Android. Version: N/A. Android ID: A-33968204. References: N-CVE-2017-0340.	2017-07-07	not yet calculated	CVE-2017-0340
				BID(link is external)
				CONFIRM(link is external)

google -- android	An information disclosure vulnerability in the NVIDIA Video Driver due to an out-of-bounds read function in the Tegra Display Controller driver could result in possible information disclosure. This issue is rated as Moderate. Product: Android. Version: N/A. Android ID: A-33718700. References: N-CVE-2017-0326.	2017-07-07	not yet calculated	CVE-2017-0326
				BID(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
heimdal -- heimdal	Heimdal before 7.4 allows remote attackers to impersonate services with Orpheus' Lyre attacks because it obtains service-principal names in a way that violates the Kerberos 5 protocol specification. In _krb5_extract_ticket() the KDC-REP service name must be obtained from the encrypted version stored in 'enc_part' instead of the unencrypted version stored in 'ticket'. Use of the unencrypted version provides an opportunity for successful server impersonation and other attacks. NOTE: this CVE is only for Heimdal and other products that embed Heimdal code; it does not apply to other instances in which this part of the Kerberos 5 protocol specification is violated.	2017-07-13	not yet calculated	CVE-2017-11103 CONFIRM CONFIRM(link is external) CONFIRM MISC(link is external) CONFIRM

ibm -- bigfix_inventory	IBM BigFix Inventory v9 9.2 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 118853.	2017-07-13	not yet calculated	CVE-2016-8964
				CONFIRM(link is external)
				MISC(link is external)

ibm -- daeja_viewone	IBM Daeja ViewONE Professional, Standard & Virtual 4.1.5.1 and 5.0 could allow an authenticated attacker to download files they should not have access to due to improper access controls. IBM X-Force ID: 125462.	2017-07-13	not yet calculated	CVE-2017-1308
				CONFIRM(link is external)
				MISC(link is external)

ibm -- emptoris_sourcing	IBM Emptoris Sourcing 9.5.x through 10.1.x is vulnerable to cross-site scripting. This vulnerability allows users to	2017-07-12	not yet calculated	CVE-2016-6114 CONFIRM(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 118352.			external) MISC(link is external)

ibm -- emptoris_sourcing	IBM Emptoris Sourcing 9.5.x through 10.1.x could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 118834	2017-07-12	not yet calculated	CVE-2016-8947
				CONFIRM(link is external)
				MISC(link is external)

ibm -- emptoris_sourcing	IBM Emptoris Sourcing 9.5.x through 10.1.x is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 118833.	2017-07-12	not yet calculated	CVE-2016-8946
				CONFIRM(link is external)
				MISC(link is external)

ibm -- emptoris_sourcing	IBM Emptoris Sourcing 9.5.x through 10.1.x is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus	2017-07-12	not yet calculated	CVE-2016-8950 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 118837.			MISC(link is external)

ibm -- emptoris_sourcing	IBM Emptoris Sourcing 9.5.x through 10.1.x is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 118835.	2017-07-12	not yet calculated	CVE-2016-8948
				CONFIRM(link is external)
				MISC(link is external)

ibm -- emptoris_sourcing	IBM Emptoris Sourcing 9.5.x through 10.1.x could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 118840.	2017-07-12	not yet calculated	CVE-2016-8953
				CONFIRM(link is external)
				MISC(link is external)

ibm -- emptoris_strategic_supply_management _platform	IBM Emptoris Strategic Supply Management Platform 10.0.0.x through 10.1.1.x is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the	2017-07-13	not yet calculated	CVE-2016-6019
				CONFIRM(link is external)
				MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 116739.			

ibm -- emptoris_strategic_supply_management_platform	IBM Emptoris Strategic Supply Management Platform 10.0.0.x through 10.1.1.x is vulnerable to a denial of service attack. An attacker can exploit a vulnerability in the authentication features that could log out users and flood user accounts with emails. IBM X-Force ID: 118838.	2017-07-13	not yet calculated	CVE-2016-8951
				CONFIRM(link is external)
				MISC(link is external)

ibm -- emptoris_strategic_supply_management_platform	IBM Emptoris Strategic Supply Management Platform 10.0.0.x through 10.1.1.x is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 118839.	2017-07-13	not yet calculated	CVE-2016-8952
				CONFIRM(link is external)
				MISC(link is external)

ibm -- websphere_commerece_enterprise	IBM WebSphere Commerce Enterprise, Professional, Express, and Developer 6.0, 7.0, and 8.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly	2017-07-10	not yet calculated	CVE-2017-1398
				CONFIRM(link is external)
				BID(link is external)
				MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sensitive information or conduct further attacks against the victim. IBM X-Force ID: 127385.			

ibm -- websphere_mq	IBM WebSphere MQ 9.0.1 and 9.0.2 could allow an authenticated user with authority to send a specially crafted message that would cause a channel to remain in a running state but not process messages. IBM X-Force ID: 125146.	2017-07-12	not yet calculated	CVE-2017-1285
				MISC(link is external)
				CONFIRM(link is external)

iceni -- infix	An out-of-bounds write vulnerability exists in the PDF parsing functionality of Infix 7.1.5. A specially crafted PDF file can cause a vulnerability resulting in potential memory corruption. An attacker can send the victim a specific PDF file to trigger this vulnerability.	2017-07-12	not yet calculated	CVE-2017-2863 MISC(link is external)
imagemagick -- imagemagick	The ReadTGAImage function in coders\tga.c in ImageMagick 7.0.5-6 has a memory leak vulnerability that can cause memory exhaustion via invalid colors data in the header of a TGA or VST file.	2017-07-11	not yet calculated	CVE-2017-11170 CONFIRM(link is external)
imagemagick -- imagemagick	The read_user_chunk_callback function in coders\png.c in ImageMagick 7.0.6-1 Q16 2017-06-21 (beta) has memory leak vulnerabilities via crafted PNG files.	2017-07-13	not yet calculated	CVE-2017-11310 CONFIRM(link is external) CONFIRM(link is external)
ipsilon -- ipsilon	A vulnerability in ipsilon 2.0 before 2.0.2, 1.2 before 1.2.1, 1.1 before 1.1.2, and 1.0 before 1.0.3 was found that allows attacker to log out active sessions of other users.	2017-07-12	not yet calculated	CVE-2016-8638 CONFIRM(link is external) CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This issue is related to how it tracks sessions, and allows an unauthenticated attacker to view and terminate active sessions from other users.			CONFIRM(link is external)

microsoft -- office	Microsoft Office allows a remote code execution vulnerability due to the way that it handles objects in memory, aka "Microsoft Office Remote Code Execution Vulnerability". This CVE ID is unique from CVE-2017-8570.	2017-07-11	not yet calculated	CVE-2017-0243
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	Microsoft WordPad in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability due to the way it parses specially crafted files, aka "WordPad Remote Code Execution Vulnerability".	2017-07-11	not yet calculated	CVE-2017-8588
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	Microsoft Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to Windows improperly handling calls to Advanced Local Procedure Call (ALPC), aka "Windows ALPC Elevation of Privilege Vulnerability".	2017-07-11	not yet calculated	CVE-2017-8562
				BID(link is external)
				CONFIRM(link is external)

microsoft -- windows	Graphics in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows	2017-07-11	not yet calculated	CVE-2017-8556 BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

	Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka "Microsoft Graphics Component Elevation of Privilege Vulnerability". This CVE ID is unique from CVE-2017-8573 and CVE-2017-8574.			SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	Windows System Information Console in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a information disclosure vulnerability improperly parses XML input containing a reference to an external entity, aka "Windows System Information Console Information Disclosure Vulnerability".	2017-07-11	not yet calculated	CVE-2017-8557
				BID(link is external)
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	Graphics in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka "Microsoft Graphics Component Elevation of Privilege	2017-07-11	not yet calculated	CVE-2017-8573
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Vulnerability". This CVE ID is unique from CVE-2017-8574 and CVE-2017-8556.			

microsoft -- windows	Windows PowerShell in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability when PSObject wraps a CIM Instance, aka "Windows PowerShell Remote Code Execution Vulnerability".	2017-07-11	not yet calculated	CVE-2017-8565
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	Graphics in Microsoft Windows 10 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability when it fails to properly handle objects in memory, aka "Microsoft Graphics Component Elevation of Privilege Vulnerability". This CVE ID is unique from CVE-2017-8573 and CVE-2017-8556.	2017-07-11	not yet calculated	CVE-2017-8574
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when it fails to properly initialize a memory address, aka "Windows Kernel Information Disclosure Vulnerability".	2017-07-11	not yet calculated	CVE-2017-8564
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

microsoft -- windows	Microsoft .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 allow an attacker to send specially crafted requests to a .NET web application, resulting in denial of service, aka .NET Denial of Service Vulnerability.	2017-07-11	not yet calculated	CVE-2017-8585
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	Microsoft Exchange Server 2010 SP3, Exchange Server 2013 SP3, Exchange Server 2013 CU16, and Exchange Server 2016 CU5 allows an open redirect vulnerability that could lead to spoofing, aka "Microsoft Exchange Open Redirect Vulnerability".	2017-07-11	not yet calculated	CVE-2017-8621
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	Windows Performance Monitor in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a information disclosure vulnerability due to the way it parses XML input, aka "Windows Performance Monitor Information Disclosure Vulnerability".	2017-07-11	not yet calculated	CVE-2017-0170
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	Internet Explorer on Microsoft Windows 8.1 and Windows RT 8.1, and Windows Server 2012 R2 allows an attacker to execute arbitrary code in the context of the current user when Internet Explorer improperly accesses objects in memory, aka "Internet	2017-07-11	not yet calculated	CVE-2017-8594
				BID(link is external)
				CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Explorer Memory Corruption Vulnerability".			

microsoft -- windows	Microsoft browsers on when Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8.1, Windows RT 8.1, and Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow a security feature bypass vulnerability when they improperly handle redirect requests, aka "Microsoft Browser Security Feature Bypass".	2017-07-11	not yet calculated	CVE-2017-8592
				BID(link is external)
				SECTRACK(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	Windows 10 1607 and Windows Server 2016 allow an attacker to execute code remotely via a specially crafted WiFi packet aka "HoloLens Remote Code Execution Vulnerability."	2017-07-11	not yet calculated	CVE-2017-8584
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	Windows Explorer in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511 allows a denial of service vulnerability when it attempts to open a non-existent file, aka "Windows Explorer Denial of Service Vulnerability".	2017-07-11	not yet calculated	CVE-2017-8587
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	HTTP.sys in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10	2017-07-11	not yet calculated	CVE-2017-8582 BID(link is external) SECTRACK(link is

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an information disclosure vulnerability when the component improperly handles objects in memory, aka "Https.sys Information Disclosure Vulnerability".			external) CONFIRM(link is external)

microsoft -- windows	Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to bypass Extended Protection for Authentication when Kerberos fails to prevent tampering with the SNAME field during ticket exchange, aka "Kerberos SNAME Security Feature Bypass Vulnerability".	2017-07-11	not yet calculated	CVE-2017-8495
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	Windows Shell in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability due to the way it improperly handles executable files and shares during rename operations, aka "Windows Explorer Remote Code Execution Vulnerability".	2017-07-11	not yet calculated	CVE-2017-8463
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

microsoft -- windows	Graphics in Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012	2017-07-11	not yet calculated	CVE-2017-8467 BID(link is external) SECTRACK

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an elevation of privilege vulnerability due to the way it handles objects in memory, aka "Win32k Elevation of Privilege Vulnerability".			(link is external) CONFIRM(link is external)

microsoft -- windows	Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows an information disclosure due to the way it handles objects in memory, aka "Win32k Information Disclosure Vulnerability".	2017-07-11	not yet calculated	CVE-2017-8486
				BID(link is external)
				SECTRACK(link is external)
				CONFIRM(link is external)

nginx -- nginx	Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.	2017-07-13	not yet calculated	CVE-2017-7529 MLIST
php_group -- php	In PHP through 5.6.31, 7.x through 7.0.21, and 7.1.x through 7.1.7, lack of bounds checks in the date extension's timelib_meridian parsing code could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-11145.	2017-07-10	not yet calculated	CVE-2017-11146 CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phpmyfaq -- phpmyfaq	phpMyFAQ before 2.9.8 does not properly mitigate brute-force attacks that try many passwords in attempted logins quickly.	2017-07-12	not yet calculated	CVE-2017-11187 CONFIRM(link is external)
poppler -- poppler	An exploitable integer overflow vulnerability exists in the JPEG 2000 image parsing functionality of freedesktop.org Poppler 0.53.0. A specially crafted PDF file can lead to an integer overflow causing out of bounds memory overwrite on the heap resulting in potential arbitrary code execution. To trigger this vulnerability, a victim must open the malicious PDF in an application using this library.	2017-07-12	not yet calculated	CVE-2017-2820 MISC(link is external)
poppler -- poppler	An exploitable heap overflow vulnerability exists in the image rendering functionality of Poppler 0.53.0. A specifically crafted PDF can cause an overly large number of color components during image rendering, resulting in heap corruption. An attacker controlled PDF file can be used to trigger this vulnerability.	2017-07-12	not yet calculated	CVE-2017-2818 MISC(link is external)
poppler -- poppler	An exploitable heap overflow vulnerability exists in the image rendering functionality of Poppler 0.53.0. A specifically crafted pdf can cause an image resizing after allocation has already occurred, resulting in heap corruption which can lead to code execution. An attacker controlled PDF file can be	2017-07-12	not yet calculated	CVE-2017-2814 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	used to trigger this vulnerability.			

project_c-ares -- c-ares	The c-ares function `ares_parse_naptr_reply()`, which is used for parsing NAPTR responses, could be triggered to read memory outside of the given input buffer if the passed in DNS response packet was crafted in a particular way.	2017-07-07	not yet calculated	CVE-2017-1000381
				BID(link is external)
				CONFIRM(link is external)
				CONFIRM(link is external)

pulse_secure -- pulse_connect_secure	Pulse Connect Secure 8.3R1 has CSRF in logout.cgi. The logout function of the admin panel is not protected by any CSRF tokens, thus allowing an attacker to logout a user by making them visit a malicious web page.	2017-07-12	not yet calculated	CVE-2017-11196 MISC(link is external) MISC(link is external)
pulse_secure -- pulse_connect_secure	Pulse Connect Secure 8.3R1 has Reflected XSS in launchHelp.cgi. The helpLaunchPage parameter is reflected in an IFRAME element, if the value contains two quotes. It properly sanitizes quotes and tags, so one cannot simply close the src with a quote and inject after that. However, an attacker can use javascript: or data: to abuse this.	2017-07-12	not yet calculated	CVE-2017-11195 MISC(link is external) MISC(link is external)
pulse_secure -- pulse_connect_secure	Pulse Connect Secure 8.3R1 has Reflected XSS in adminservercacertdetails.cgi. In the admin panel, the certid parameter of adminservercacertdetails.cgi is reflected in the application's response and is not properly sanitized, allowing an attacker to inject tags. An attacker could come up with clever	2017-07-12	not yet calculated	CVE-2017-11194 MISC(link is external) MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	payloads to make the system run commands such as ping, ping6, traceroute, nslookup, arp, etc.			
pulse_secure -- pulse_connect_secure	Pulse Connect Secure 8.3R1 has CSRF in diag.cgi. In the panel, the diag.cgi file is responsible for running commands such as ping, ping6, traceroute, traceroute6, nslookup, arp, and Portprobe. These functions do not have any protections against CSRF. That can allow an attacker to run these commands against any IP if they can get an admin to visit their malicious CSRF page.	2017-07-12	not yet calculated	CVE-2017-11193 MISC(link is external) MISC(link is external)
rack-cors -- rack-cors	Missing anchor in generated regex for rack-cors before 0.4.1 allows a malicious third-party site to perform CORS requests. If the configuration were intended to allow only the trusted example.com domain name and not the malicious example.net domain name, then example.com.example.net (as well as example.com-example.net) would be inadvertently allowed.	2017-07-12	not yet calculated	CVE-2017-11173 MISC MISC(link is external) MISC(link is external)
sap -- netweaver	SAP NetWeaver 7400.12.21.30308 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted serialized Java object in a request to metadatauploader, aka SAP Security Note 2399804.	2017-07-12	not yet calculated	CVE-2017-9844 MISC(link is external)
sap -- netweaver	SAP NetWeaver AS ABAP 7.40 allows remote authenticated users with	2017-07-12	not yet calculated	CVE-2017-9843

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	certain privileges to cause a denial of service (process crash) via vectors involving disp+work.exe, aka SAP Security Note 2406841.			MISC(link is external)
sap -- netweaver	disp+work 7400.12.21.30308 in SAP NetWeaver 7.40 allows remote attackers to cause a denial of service (resource consumption) via a crafted DIAG request, aka SAP Security Note 2405918.	2017-07-12	not yet calculated	CVE-2017-9845 MISC(link is external)

siemens -- simatic_cp_44x-1_rna	An Improper Authentication issue was discovered in Siemens SIMATIC CP 44x-1 RNA, all versions prior to 1.4.1. An unauthenticated remote attacker may be able to perform administrative actions on the Communication Process (CP) of the RNA series module, if network access to Port 102/TCP is available and the configuration file for the CP is stored on the RNA's CPU.	2017-07-07	not yet calculated	CVE-2017-6868
				BID(link is external)
				SECTRACK(link is external)
				MISC

thermo_fisher_scientific -- datataker_dt80_dex	dataTaker DT80 dEX 1.50.012 allows remote attackers to obtain sensitive credential and configuration information via a direct request for the /services/getFile.cmd?userfile=config.xml URI.	2017-07-12	not yet calculated	CVE-2017-11165 MISC(link is external)
unrar-free -- unrar-free	unrarlib.c in unrar-free 0.0.1, when _DEBUG_LOG mode is enabled, might allow remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via an RAR archive containing a long filename.	2017-07-12	not yet calculated	CVE-2017-11190 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
unrar-free -- unrar-free	unrarlib.c in unrar-free 0.0.1 might allow remote attackers to cause a denial of service (NULL pointer dereference and application crash), which could be relevant if unrarlib is used as library code for a long-running application.	2017-07-12	not yet calculated	CVE-2017-11189 MISC(link is external)
xoops -- xoops	In install/page_dbsettings.php in the Core distribution of XOOPS 2.5.8.1, unfiltered data passed to CREATE and ALTER SQL queries caused SQL Injection in the database settings page, related to use of GBK in CHARACTER SET and COLLATE clauses.	2017-07-12	not yet calculated	CVE-2017-11174 MISC(link is external)