Bulletin (SB17-142)

Vulnerability Summary for the Week of May 15, 2017

Original release date: May 22, 2017

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

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

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
google -- android	An elevation of privilege vulnerability in the MediaTek touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: N/A. Android ID: A -30202412 . References: M-ALPS 02897901 .	2017-05-12	9.3	CVE-2016-10274 CONFIRM
google -- android	An elevation of privilege vulnerability in the Qualcomm bootloader could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: N/A. Android ID: A -34514954 . References: QC-CR# 1009111 .	2017-05-12	9.3	CVE-2016-10275 BID CONFIRM
google -- android	An elevation of privilege vulnerability in the Qualcomm bootloader could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: N/A. Android ID: A -32952839 . References: QC-CR# 1094105 .	2017-05-12	9.3	CVE-2016-10276 BID CONFIRM
google -- android	An elevation of privilege vulnerability in the MediaTek thermal driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A -28175767 . References: M-ALPS 02696445 .	2017-05-12	7.6	CVE-2016-10280 CONFIRM
google -- android	An elevation of privilege vulnerability in the MediaTek thermal driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A -28175647 . References: M-ALPS 02696475 .	2017-05-12	7.6	CVE-2016-10281 CONFIRM
google -- android	An elevation of privilege vulnerability in the MediaTek thermal driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A -33939045 . References: M-ALPS 03149189 .	2017-05-12	7.6	CVE-2016-10282 CONFIRM
google -- android	A remote code execution vulnerability in libmpeg2 in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -35219737 .	2017-05-12	9.3	CVE-2017-0587 BID CONFIRM CONFIRM
google -- android	A remote code execution vulnerability in id3/ID3.cpp in libstagefright in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -34618607 .	2017-05-12	9.3	CVE-2017-0588 BID CONFIRM CONFIRM
google -- android	A remote code execution vulnerability in libhevc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -34897036 .	2017-05-12	9.3	CVE-2017-0589 BID CONFIRM CONFIRM
google -- android	A remote code execution vulnerability in libhevc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -35039946 .	2017-05-12	9.3	CVE-2017-0590 BID CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	A remote code execution vulnerability in libavc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -34097672 .	2017-05-12	9.3	CVE-2017-0591 BID CONFIRM CONFIRM
google -- android	A remote code execution vulnerability in FLACExtractor.cpp in libstagefright in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -34970788 .	2017-05-12	9.3	CVE-2017-0592 BID CONFIRM CONFIRM
google -- android	An elevation of privilege vulnerability in the Framework APIs could enable a local malicious application to obtain access to custom permissions. This issue is rated as High because it is a general bypass for operating system protections that isolate application data from other applications. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -34114230 .	2017-05-12	9.3	CVE-2017-0593 BID CONFIRM
google -- android	An elevation of privilege vulnerability in codecs/aacenc/SoftAACEncoder2.cpp in libstagefright in Mediaserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -34617444 .	2017-05-12	9.3	CVE-2017-0594 BID CONFIRM CONFIRM
google -- android	An elevation of privilege vulnerability in libstagefright in Mediaserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A -34705519 .	2017-05-12	9.3	CVE-2017-0595 BID CONFIRM CONFIRM
google -- android	An elevation of privilege vulnerability in libstagefright in Mediaserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A -34749392 .	2017-05-12	9.3	CVE-2017-0596 BID CONFIRM CONFIRM
google -- android	An elevation of privilege vulnerability in Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -34749571 .	2017-05-12	9.3	CVE-2017-0597 BID CONFIRM
google -- android	A remote denial of service vulnerability in libhevc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -34672748 .	2017-05-12	7.1	CVE-2017-0599 BID CONFIRM CONFIRM
google -- android	A remote denial of service vulnerability in libstagefright in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -35269635 .	2017-05-12	7.1	CVE-2017-0600 CONFIRM CONFIRM
google -- android	An elevation of privilege vulnerability in the kernel Qualcomm power driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: N/A. Android ID: A-35392981. References: QC-CR#826589.	2017-05-12	9.3	CVE-2017-0604 CONFIRM
google -- android	An elevation of privilege vulnerability in the MediaTek power driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A -34259126 . References: M-ALPS 03150278 .	2017-05-12	7.6	CVE-2017-0615 BID CONFIRM
google -- android	An elevation of privilege vulnerability in the MediaTek system management interrupt driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A -34470286 . References: M-ALPS 03149160 .	2017-05-12	7.6	CVE-2017-0616 BID CONFIRM
google -- android	An elevation of privilege vulnerability in the MediaTek video driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A -34471002 . References: M-ALPS 03149173 .	2017-05-12	7.6	CVE-2017-0617 BID CONFIRM
google -- android	An elevation of privilege vulnerability in the MediaTek command queue driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A -35100728 . References: M-ALPS 03161536 .	2017-05-12	7.6	CVE-2017-0618 CONFIRM
google -- android	An elevation of privilege vulnerability in the Qualcomm pin controller driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-35401152. References: QC-CR#826566.	2017-05-12	7.6	CVE-2017-0619 BID CONFIRM
google -- android	An elevation of privilege vulnerability in the Qualcomm Secure Channel Manager driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -35401052 . References: QC-CR# 1081711 .	2017-05-12	7.6	CVE-2017-0620 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	A remote denial of service vulnerability in HevcUtils.cpp in libstagefright in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as Low due to details specific to the vulnerability. Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID: A -35467107 .	2017-05-12	7.1	CVE-2017-0635 CONFIRM CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Motorola bootloader could enable a local malicious application to execute arbitrary code within the context of the bootloader. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -33840490 .	2017-05-12	9.3	CVE-2016-10277 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -32094986 . References: QC-CR# 2002052 .	2017-05-12	7.6	CVE-2016-10283 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm video driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -32402303 . References: QC-CR# 2000664 .	2017-05-12	7.6	CVE-2016-10284 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm video driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A -33752702 . References: QC-CR# 1104899 .	2017-05-12	7.6	CVE-2016-10285 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm video driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A -35400904 . References: QC-CR# 1090237 .	2017-05-12	7.6	CVE-2016-10286 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -33784446 . References: QC-CR# 1112751 .	2017-05-12	7.6	CVE-2016-10287 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm LED driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A -33863909 . References: QC-CR# 1109763 .	2017-05-12	7.6	CVE-2016-10288 CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm crypto driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -33899710 . References: QC-CR# 1116295 .	2017-05-12	7.6	CVE-2016-10289 CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm shared memory driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -33898330 . References: QC-CR# 1109782 .	2017-05-12	7.6	CVE-2016-10290 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Slimbus driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-34030871. References: QC-CR#986837.	2017-05-12	7.6	CVE-2016-10291 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm ADSPRPC driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -34112914 . References: QC-CR# 1110747 .	2017-05-12	7.6	CVE-2017-0465 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the kernel trace subsystem could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -35399704 . References: QC-CR# 1048480 .	2017-05-12	9.3	CVE-2017-0605 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -34088848 . References: QC-CR# 1116015 .	2017-05-12	7.6	CVE-2017-0606 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A -35400551 . References: QC-CR# 1085928 .	2017-05-12	7.6	CVE-2017-0607 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -35400458 . References: QC-CR# 1098363 .	2017-05-12	7.6	CVE-2017-0608 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -35399801 . References: QC-CR# 1090482 .	2017-05-12	7.6	CVE-2017-0609 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -35399404 . References: QC-CR# 1094852 .	2017-05-12	7.6	CVE-2017-0610 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -35393841 . References: QC-CR# 1084210 .	2017-05-12	7.6	CVE-2017-0611 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Secure Execution Environment Communicator driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A -34389303 . References: QC-CR# 1061845 .	2017-05-12	7.6	CVE-2017-0612 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Secure Execution Environment Communicator driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -35400457 . References: QC-CR# 1086140 .	2017-05-12	7.6	CVE-2017-0613 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Secure Execution Environment Communicator driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -35399405 . References: QC-CR# 1080290 .	2017-05-12	7.6	CVE-2017-0614 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm camera driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-35399703. References: QC-CR#831322.	2017-05-12	7.6	CVE-2017-0621 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Goodix touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A -32749036 . References: QC-CR# 1098602 .	2017-05-12	7.6	CVE-2017-0622 BID CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the HTC bootloader could enable a local malicious application to execute arbitrary code within the context of the bootloader. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A -32512358 .	2017-05-12	7.6	CVE-2017-0623 BID CONFIRM
tnef_project -- tnef	An integer underflow has been identified in the unicode_to_utf8() function in tnef 1.4.14. This might lead to invalid write operations, controlled by an attacker.	2017-05-12	7.5	CVE-2017-8911 MISC

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adodb_project -- adodb	Cross-site scripting vulnerability in ADOdb versions prior to 5.20.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-05-12	4.3	CVE-2016-4855 JVN BID CONFIRM
artifex -- ghostscript	The mark_line_tr function in gxscanc.c in Artifex Ghostscript 9.21 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PostScript document.	2017-05-12	4.3	CVE-2017-8908 MISC
basercms -- basercms	Cross-site request forgery (CSRF) vulnerability in baserCMS version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators to execute arbitrary PHP code via unspecified vectors.	2017-05-12	6.8	CVE-2016-4876 MISC BID JVN
basercms -- basercms	Cross-site request forgery (CSRF) vulnerability in baserCMS version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2017-05-12	6.8	CVE-2016-4878 CONFIRM BID JVN
basercms -- basercms	Cross-site request forgery (CSRF) vulnerability in baserCMS plugin Mail version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2017-05-12	6.8	CVE-2016-4879 CONFIRM BID JVN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
basercms -- basercms	Cross-site request forgery (CSRF) vulnerability in baserCMS plugin Blog version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2017-05-12	6.8	CVE-2016-4881 CONFIRM BID JVN
basercms -- basercms	Cross-site request forgery (CSRF) vulnerability in baserCMS version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2017-05-12	6.8	CVE-2016-4882 CONFIRM BID JVN
basercms -- basercms	Cross-site request forgery (CSRF) vulnerability in baserCMS plugin Blog version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2017-05-12	6.8	CVE-2016-4884 CONFIRM BID JVN
basercms -- basercms	Cross-site request forgery (CSRF) vulnerability in baserCMS plugin Feed version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2017-05-12	6.8	CVE-2016-4885 CONFIRM BID JVN
basercms -- basercms	Cross-site request forgery (CSRF) vulnerability in baserCMS plugin Mail version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2017-05-12	6.8	CVE-2016-4886 CONFIRM BID JVN
basercms -- basercms	Cross-site request forgery (CSRF) vulnerability in baserCMS plugin Uploader version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2017-05-12	6.8	CVE-2016-4887 CONFIRM BID JVN
cmsmadesimple -- cms_made_simple	** DISPUTED ** CMS Made Simple (CMSMS) 2.1.6 allows remote authenticated administrators to execute arbitrary PHP code via the code parameter to admin/editusertag.php, related to the CreateTagFunction and CallUserTag functions. NOTE: the vendor reportedly has stated this is "a feature, not a bug."	2017-05-12	6.5	CVE-2017-8912 MISC
google -- android	An information disclosure vulnerability in File-Based Encryption could enable a local malicious attacker to bypass operating system protections for the lock screen. This issue is rated as Moderate due to the possibility of bypassing the lock screen. Product: Android. Versions: 7.0, 7.1.1. Android ID: A -32793550 .	2017-05-12	4.3	CVE-2017-0493 BID CONFIRM
google -- android	An information disclosure vulnerability in the Framework APIs could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -34128677 .	2017-05-12	4.3	CVE-2017-0598 BID CONFIRM
google -- android	An Elevation of Privilege vulnerability in Bluetooth could potentially enable a local malicious application to accept harmful files shared via bluetooth without user permission. This issue is rated as Moderate due to local bypass of user interaction requirements. Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID: A -35258579 .	2017-05-12	4.3	CVE-2017-0601 BID CONFIRM
google -- android	An information disclosure vulnerability in Bluetooth could allow a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as Moderate due to details specific to the vulnerability. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -34946955 .	2017-05-12	4.3	CVE-2017-0602 BID CONFIRM
google -- android	A denial of service vulnerability in libstagefright in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as Moderate because it requires an uncommon device configuration. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A -35763994 .	2017-05-12	5.4	CVE-2017-0603 BID CONFIRM CONFIRM
google -- android	An information disclosure vulnerability in the MediaTek command queue driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it could be used to access sensitive data without explicit user permission. Product: Android. Versions: N/A. Android ID: A -35142799 . References: M-ALPS 03161531 .	2017-05-12	4.3	CVE-2017-0625 CONFIRM
linux -- linux_kernel	A denial of service vulnerability in the Qualcomm Wi-Fi driver could enable a proximate attacker to cause a denial of service in the Wi-Fi subsystem. This issue is rated as High due to the possibility of remote denial of service. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -34514463 . References: QC-CR# 1065466 .	2017-05-12	4.3	CVE-2016-10292 BID CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it could be used to access sensitive data without explicit user permission. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -34327795 . References: QC-CR# 2005832 .	2017-05-12	4.3	CVE-2017-0624 BID CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm crypto engine driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it could be used to access sensitive data without explicit user permission. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -35393124 . References: QC-CR# 1088050 .	2017-05-12	4.3	CVE-2017-0626 BID CONFIRM
softbank -- primedrive_desktop_application	Untrusted search path vulnerability in Installer for PrimeDrive Desktop Application version 1.4.4 and earlier allows remote attackers to execute arbitrary code via a specially crafted executable file in an unspecified directory.	2017-05-12	6.8	CVE-2017-2167 MISC JVN
splunk -- splunk	Open redirect vulnerability in Splunk Enterprise 6.4.x prior to 6.4.2, Splunk Enterprise 6.3.x prior to 6.3.6, Splunk Enterprise 6.2.x prior to 6.2.11 and Splunk Light prior to 6.4.2 allows to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2017-05-12	5.8	CVE-2016-4857 JVN CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
splunk -- splunk	Open redirect vulnerability in Splunk Enterprise 6.4.x prior to 6.4.3, Splunk Enterprise 6.3.x prior to 6.3.6, Splunk Enterprise 6.2.x prior to 6.2.10, Splunk Enterprise 6.1.x prior to 6.1.11, Splunk Enterprise 6.0.x prior to 6.0.12, Splunk Enterprise 5.0.x prior to 5.0.16 and Splunk Light prior to 6.4.3 allows to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2017-05-12	5.8	CVE-2016-4859 BID JVN CONFIRM

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
basercms -- basercms	Cross-site scripting vulnerability in baserCMS plugin Mail version 3.0.10 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-05-12	3.5	CVE-2016-4877 CONFIRM BID JVN
basercms -- basercms	Cross-site scripting vulnerability in baserCMS plugin Blog version 3.0.10 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-05-12	3.5	CVE-2016-4880 CONFIRM BID JVN
basercms -- basercms	Cross-site scripting vulnerability in baserCMS version 3.0.10 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-05-12	3.5	CVE-2016-4883 CONFIRM BID JVN
conexant -- mictray64	Conexant Systems mictray64 task, as used on HP Elite, EliteBook, ProBook, and ZBook systems, leaks sensitive data (keystrokes) to any process. In mictray64.exe (mic tray icon) 1.0.0.46, a LowLevelKeyboardProc Windows hook is used to capture keystrokes. This data is leaked via unintended channels: debug messages accessible to any process that is running in the current user session, and filesystem access to C:\Users\Public\MicTray.log by any process.	2017-05-12	2.1	CVE-2017-8360 MISC MISC
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm video driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A -33352393 . References: QC-CR# 1101943 .	2017-05-12	2.6	CVE-2016-10293 BID CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm power driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -33621829 . References: QC-CR# 1105481 .	2017-05-12	2.6	CVE-2016-10294 CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm LED driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A -33781694 . References: QC-CR# 1109326 .	2017-05-12	2.6	CVE-2016-10295 CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm shared memory driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -33845464 . References: QC-CR# 1109782 .	2017-05-12	2.6	CVE-2016-10296 CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the kernel UVC driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -33300353 .	2017-05-12	2.6	CVE-2017-0627 BID CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm camera driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -34230377 . References: QC-CR# 1086833 .	2017-05-12	2.6	CVE-2017-0628 BID CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm camera driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -35214296 . References: QC-CR# 1086833 .	2017-05-12	2.6	CVE-2017-0629 BID CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the kernel trace subsystem could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -34277115 .	2017-05-12	2.6	CVE-2017-0630 BID CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm camera driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A -35399756 . References: QC-CR# 1093232 .	2017-05-12	2.6	CVE-2017-0631 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm sound codec driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-35392586. References: QC-CR#832915.	2017-05-12	2.6	CVE-2017-0632 BID CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Broadcom Wi-Fi driver could enable a local malicious component to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-36000515. References: B-RB#117131.	2017-05-12	2.6	CVE-2017-0633 BID CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Synaptics touchscreen driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A -32511682 .	2017-05-12	2.6	CVE-2017-0634 BID CONFIRM
linux -- linux_kernel	The edge_bulk_in_callback function in drivers/usb/serial/io_ti.c in the Linux kernel before 4.10.4 allows local users to obtain sensitive information (in the dmesg ringbuffer and syslog) from uninitialized kernel memory by using a crafted USB device (posing as an io_ti USB serial device) to trigger an integer underflow.	2017-05-12	2.1	CVE-2017-8924 CONFIRM CONFIRM CONFIRM
linux -- linux_kernel	The omninet_open function in drivers/usb/serial/omninet.c in the Linux kernel before 4.10.4 allows local users to cause a denial of service (tty exhaustion) by leveraging reference count mishandling.	2017-05-12	2.1	CVE-2017-8925 CONFIRM CONFIRM CONFIRM
splunk -- splunk	Cross-site scripting vulnerability in Splunk Enterprise 6.3.x prior to 6.3.5 and Splunk Light 6.3.x prior to 6.3.5 allows attacker with administrator rights to inject arbitrary web script or HTML via unspecified vectors.	2017-05-12	3.5	CVE-2016-4856 BID JVN CONFIRM
splunk -- splunk	Cross-site scripting vulnerability in Splunk Enterprise 6.4.x prior to 6.4.2, Splunk Enterprise 6.3.x prior to 6.3.6, Splunk Enterprise 6.2.x prior to 6.2.10, Splunk Enterprise 6.1.x prior to 6.1.11, Splunk Enterprise 6.0.x prior to 6.0.12, Splunk Enterprise 5.0.x prior to 5.0.16 and Splunk Light prior to 6.4.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-05-12	3.5	CVE-2016-4858 JVN CONFIRM
tenable -- nessus	Cross-site scripting vulnerability in Nessus versions 6.8.0, 6.8.1, 6.9.0, 6.9.1 and 6.9.2 allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-05-12	3.5	CVE-2017-2122 JVN CONFIRM

Back to top

Severity Not Yet Assigned				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
3s smart_software_solutions -- web_server	An Arbitrary File Upload issue was discovered in 3S-Smart Software Solutions GmbH CODESYS Web Server. The following versions of CODESYS Web Server, part of the CODESYS WebVisu web browser visualization software, are affected: CODESYS Web Server Versions 2.3 and prior. A specially crafted web server request may allow the upload of arbitrary files (with a dangerous type) to the CODESYS Web Server without authorization which may allow remote code execution.	2017-05-18	not yet calculated	CVE-2017-6027 BID MISC
3s_smart_software_solutions -- web_server	A Stack Buffer Overflow issue was discovered in 3S-Smart Software Solutions GmbH CODESYS Web Server. The following versions of CODESYS Web Server, part of the CODESYS WebVisu web browser visualization software, are affected: CODESYS Web Server Versions 2.3 and prior. A malicious user could overflow the stack buffer by providing overly long strings to functions that handle the XML. Because the function does not verify string size before copying to memory, the attacker may then be able to crash the application or run arbitrary code.	2017-05-18	not yet calculated	CVE-2017-6025 BID MISC
admidio -- csrf	admidio 3.2.8 has CSRF in adm_program/modules/members/members_function.php with an impact of deleting arbitrary user accounts.	2017-05-16	not yet calculated	CVE-2017-8382 EXPLOIT-DB
allen_disk -- reg.php	/admin/loginc.php in Allen Disk 1.6 doesn't check if isset($_SESSION['captcha']['code']) == 1, which leads to CAPTCHA bypass by emptying $_POST['captcha'].	2017-05-19	not yet calculated	CVE-2017-9091 CONFIRM
allen_disk -- reg.php	reg.php in Allen Disk 1.6 doesn't check if isset($_SESSION['captcha']['code'])==1, which makes it possible to bypass the CAPTCHA via an empty $_POST['captcha'].	2017-05-19	not yet calculated	CVE-2017-9090 CONFIRM
ambari -- server_host	In Ambari 2.2.2 through 2.4.2 and Ambari 2.5.0, sensitive data may be stored on disk in temporary files on the Ambari Server host. The temporary files are readable by any user authenticated on the host.	2017-05-15	not yet calculated	CVE-2017-5655 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache-- cxf_fediz_ship	Apache CXF Fediz ships with an OpenId Connect (OIDC) service which has a Client Registration Service, which is a simple web application that allows clients to be created, deleted, etc. A CSRF (Cross Style Request Forgery) style vulnerability has been found in this web application in Apache CXF Fediz prior to 1.4.0 and 1.3.2, meaning that a malicious web application could create new clients, or reset secrets, etc, after the admin user has logged on to the client registration service and the session is still active.	2017-05-16	not yet calculated	CVE-2017-7662 CONFIRM
apache-- cxf_fediz_ship	Apache CXF Fediz ships with a number of container-specific plugins to enable WS-Federation for applications. A CSRF (Cross Style Request Forgery) style vulnerability has been found in the Spring 2, Spring 3, Jetty 8 and Jetty 9 plugins in Apache CXF Fediz prior to 1.4.0, 1.3.2 and 1.2.4.	2017-05-16	not yet calculated	CVE-2017-7661 CONFIRM
apache -- juddi	After logging into the portal, the logout jsp page redirects the browser back to the login page after. It is feasible for malicious users to redirect the browser to an unintended web page in Apache jUDDI 3.1.2, 3.1.3, 3.1.4, and 3.1.5 when utilizing the portlets based user interface also known as 'Pluto', 'jUDDI Portal', 'UDDI Portal' or 'uddi-console'. User session data, credentials, and auth tokens are cleared before the redirect.	2017-05-19	not yet calculated	CVE-2015-5241 MISC
apache -- qpid_broker	The Apache Qpid Broker for Java can be configured to use different so called AuthenticationProviders to handle user authentication. Among the choices are the SCRAM-SHA-1 and SCRAM-SHA-256 AuthenticationProvider types. It was discovered that these AuthenticationProviders in Apache Qpid Broker for Java 6.0.x before 6.0.6 and 6.1.x before 6.1.1 prematurely terminate the SCRAM SASL negotiation if the provided user name does not exist thus allowing remote attacker to determine the existence of user accounts. The Vulnerability does not apply to AuthenticationProviders other than SCRAM-SHA-1 and SCRAM-SHA-256.	2017-05-15	not yet calculated	CVE-2016-8741 MLIST BID CONFIRM
authconfig -- sssd	Authconfig version 6.2.8 is vulnerable to an Information exposure while using SSSD to authenticate against remote server resulting in the leak of information about existing usernames.	2017-05-16	not yet calculated	CVE-2017-7488 CONFIRM CONFIRM
cairo -- ft_load__render_glyph_	Cairo version 1.15.4 is vulnerable to a NULL pointer dereference related to the FT_Load_Glyph and FT_Render_Glyph resulting in an application crash.	2017-05-19	not yet calculated	CVE-2017-7475 MLIST MISC MISC
calendarxp -- flatcalendarxp	Two CalendarXP products have XSS in common parts of HTML files. CalendarXP FlatCalendarXP through 9.9.290 has XSS in iflateng.htm and nflateng.htm. CalendarXP PopCalendarXP through 9.8.308 has XSS in ipopeng.htm and npopeng.htm.	2017-05-18	not yet calculated	CVE-2017-9072 MISC
cisco -- aironet	A vulnerability in the Plug-and-Play (PnP) subsystem of the Cisco Aironet 1800, 2800, and 3800 Series Access Points running a Lightweight Access Point (AP) or Mobility Express image could allow an unauthenticated, adjacent attacker to execute arbitrary code with root privileges. The vulnerability is due to insufficient validation of PnP server responses. The PnP feature is only active while the device does not contain a configuration, such as a first time boot or after a factory reset has been issued. An attacker with the ability to respond to PnP configuration requests from the affected device can exploit the vulnerability by returning malicious PnP responses. If a Cisco Application Policy Infrastructure Controller - Enterprise Module (APIC-EM) is available on the network, the attacker would need to exploit the issue in the short window before a valid PnP response was received. If successful, the attacker could gain the ability to execute arbitrary code with root privileges on the underlying operating system of the device. Cisco has confirmed that the only vulnerable software version is 8.3.102.0. Cisco Bug IDs: CSCvb42386.	2017-05-16	not yet calculated	CVE-2017-3873 BID CONFIRM
cisco -- ios_xr	A vulnerability in the Event Management Service daemon (emsd) of Cisco IOS XR routers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the affected device. The vulnerability is due to improper handling of gRPC requests. An attacker could exploit this vulnerability by repeatedly sending unauthenticated gRPC requests to the affected device. A successful exploit could allow the attacker to crash the device in such a manner that manual intervention is required to recover. This vulnerability affects all Cisco IOS XR platforms that are running release 6.1.1 of Cisco IOS XR Software when the gRPC service is enabled on the device. The gRPC service is not enabled by default. Cisco Bug IDs: CSCvb14441.	2017-05-16	not yet calculated	CVE-2017-3876 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- policy_suite	A vulnerability in a script file that is installed as part of the Cisco Policy Suite (CPS) Software distribution for the CPS appliance could allow an authenticated, local attacker to escalate their privilege level to root. The vulnerability is due to incorrect sudoers permissions on the script file. An attacker could exploit this vulnerability by authenticating to the device and providing crafted user input at the CLI, using this script file to escalate their privilege level and execute commands as root. A successful exploit could allow the attacker to acquire root-level privileges and take full control of the appliance. The user has to be logged-in to the device with valid credentials for a specific set of users. The Cisco Policy Suite application is vulnerable when running software versions 10.0.0, 10.1.0, or 11.0.0. Cisco Bug IDs: CSCvc07366.	2017-05-18	not yet calculated	CVE-2017-6623 CONFIRM
cisco -- router	A vulnerability in the Universal Plug-and-Play (UPnP) implementation in the Cisco CVR100W Wireless-N VPN Router could allow an unauthenticated, Layer 2-adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition. The remote code execution could occur with root privileges. The vulnerability is due to incomplete range checks of the UPnP input data, which could result in a buffer overflow. An attacker could exploit this vulnerability by sending a malicious request to the UPnP listening port of the targeted device. An exploit could allow the attacker to cause the device to reload or potentially execute arbitrary code with root privileges. This vulnerability affects all firmware releases of the Cisco CVR100W Wireless-N VPN Router prior to Firmware Release 1.0.1.22. Cisco Bug IDs: CSCuz72642.	2017-05-16	not yet calculated	CVE-2017-3882 BID CONFIRM
cisco -- sourcefire_snort	Cisco Sourcefire Snort 3.0 before build 233 has a Buffer Overread related to use of a decoder array. The size was off by one making it possible to read past the end of the array with an ether type of 0xFFFF. Increasing the array size solves this problem.	2017-05-16	not yet calculated	CVE-2017-6658 CONFIRM
cisco -- sourcefire_snort	Cisco Sourcefire Snort 3.0 before build 233 mishandles Ether Type Validation. Since valid ether type and IP protocol numbers do not overlap, Snort++ stores all protocol decoders in a single array. That makes it possible to craft packets that have IP protocol numbers in the ether type field which will confuse the Snort++ decoder. For example, an eth:llc:snap:icmp6 packet will cause a crash because there is no ip6 header with which to calculate the icmp6 checksum. Affected decoders include gre, llc, trans_bridge, ciscometadata, linux_sll, and token_ring. The fix adds a check in the packet manager to validate the ether type before indexing the decoder array. An out of range ether type will raise 116:473.	2017-05-16	not yet calculated	CVE-2017-6657 CONFIRM
cisco -- telepresence	A vulnerability in the ICMP ingress packet processing of Cisco TelePresence Collaboration Endpoint (CE) Software could allow an unauthenticated, remote attacker to cause the TelePresence endpoint to reload unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to incomplete input validation for the size of a received ICMP packet. An attacker could exploit this vulnerability by sending a crafted ICMP packet to the local IP address of the targeted endpoint. A successful exploit could allow the attacker to cause a DoS of the TelePresence endpoint, during which time calls could be dropped. This vulnerability would affect either IPv4 or IPv6 ICMP traffic. This vulnerability affects the following Cisco TelePresence products when running software release CE8.1.1, CE8.2.0, CE8.2.1, CE8.2.2, CE 8.3.0, or CE8.3.1: Spark Room OS, TelePresence DX Series, TelePresence MX Series, TelePresence SX Quick Set Series, TelePresence SX Series. Cisco Bug IDs: CSCvb95396.	2017-05-16	not yet calculated	CVE-2017-3825 BID CONFIRM
cisco -- telepresence	A vulnerability in the web framework of the Cisco TelePresence IX5000 Series could allow an unauthenticated, remote attacker to access arbitrary files on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by using directory traversal techniques to read files within the Cisco TelePresence IX5000 Series filesystem. This vulnerability affects Cisco TelePresence IX5000 Series devices running software version 8.2.0. Cisco Bug IDs: CSCvc52325.	2017-05-18	not yet calculated	CVE-2017-6652 CONFIRM
cisco -- web_interface	A vulnerability in the web interface for Cisco Prime Collaboration Provisioning could allow an unauthenticated, remote attacker to bypass authentication and perform command injection with root privileges. The vulnerability is due to missing security constraints in certain HTTP request methods, which could allow access to files via the web interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to the targeted application. This vulnerability affects Cisco Prime Collaboration Provisioning Software Releases prior to 12.1. Cisco Bug IDs: CSCvc98724.	2017-05-18	not yet calculated	CVE-2017-6622 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- web_interface	A vulnerability in the web interface of Cisco Prime Collaboration Provisioning could allow an unauthenticated, remote attacker to access sensitive data. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to insufficient protection of sensitive data when responding to an HTTP request on the web interface. An attacker could exploit the vulnerability by sending a crafted HTTP request to the application to access specific system files. An exploit could allow the attacker to obtain sensitive information about the application which could include user credentials. This vulnerability affects Cisco Prime Collaboration Provisioning Software Releases 10.6 through 11.5. Cisco Bug IDs: CSCvc99626.	2017-05-18	not yet calculated	CVE-2017-6621 CONFIRM
cisco -- webex	A vulnerability in Cisco WebEx Meetings Server could allow unauthenticated, remote attackers to gain information that could allow them to access scheduled customer meetings. The vulnerability is due to an incomplete configuration of the robots.txt file on customer-hosted WebEx solutions and occurs when the Short URL functionality is not activated. All releases of Cisco WebEx Meetings Server later than release 2.5MR4 provide this functionality. An attacker could exploit this vulnerability via an exposed parameter to search for indexed meeting information. A successful exploit could allow the attacker to obtain scheduled meeting information and potentially allow the attacker to attend scheduled, customer meetings. This vulnerability affects the following releases of Cisco WebEx Meetings Server: 2.5, 2.6, 2.7, 2.8. Cisco Bug IDs: CSCve25950.	2017-05-16	not yet calculated	CVE-2017-6651 BID CONFIRM
deluge -- webui	The WebUI component in Deluge before 1.3.15 contains a directory traversal vulnerability involving a request in which the name of the render file is not associated with any template file.	2017-05-17	not yet calculated	CVE-2017-9031 CONFIRM CONFIRM CONFIRM
dropbear -- server	Dropbear before 2017.75 might allow local users to read certain files as root, if the file has the authorized_keys file format with a command= option. This occurs because ~/.ssh/authorized_keys is read with root privileges and symlinks are followed.	2017-05-19	not yet calculated	CVE-2017-9079 CONFIRM
dropbear -- server	The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.	2017-05-19	not yet calculated	CVE-2017-9078 CONFIRM
edgewater -- networks_edgemarc	The HTTP web-management application on Edgewater Networks Edgemarc appliances has a hidden page that allows for user-defined commands such as specific iptables routes, etc., to be set. You can use this page as a web shell essentially to execute commands, though you get no feedback client-side from the web application: if the command is valid, it executes. An example is the wget command. The page that allows this has been confirmed in firmware as old as 2006.	2017-05-16	not yet calculated	CVE-2017-6079 MISC
eir -- d1000	The Eir D1000 modem does not properly restrict the TR-064 protocol, which allows remote attackers to execute arbitrary commands via TCP port 7547, as demonstrated by opening WAN access to TCP port 80, retrieving the login password (which defaults to the Wi-Fi password), and using the NewNTPServer feature.	2017-05-16	not yet calculated	CVE-2016-10372 MISC MISC
emc -- isilon_onefs	EMC Isilon OneFS 8.0.1.0, OneFS 8.0.0.0 - 8.0.0.2, OneFS 7.2.1.0 - 7.2.1.3, and OneFS 7.2.0.x is affected by an NFS export vulnerability. Under certain conditions, after upgrading a cluster from OneFS 7.1.1.x or earlier, users may have unexpected levels of access to some NFS exports.	2017-05-19	not yet calculated	CVE-2017-4979 CONFIRM
emc -- rsa_adaptive_authentication	EMC RSA Adaptive Authentication (On-Premise) versions prior to 7.3 P2 (exclusive) contains a fix for a cross-site scripting vulnerability that could potentially be exploited by malicious users to compromise the affected system.	2017-05-19	not yet calculated	CVE-2017-4978 CONFIRM
flexnet -- manager_suite	An error when handling certain external commands and services related to the FlexNet Inventory Agent and FlexNet Beacon of the Flexera Software FlexNet Manager Suite 2017 before 2017 R1 and 2014 R3 through 2016 R1 SP1 can be exploited to gain elevated privileges.	2017-05-16	not yet calculated	CVE-2017-6885 MISC
geutebruck -- ip_camera	An Authentication Bypass issue was discovered in Geutebruck IP Camera G-Cam/EFD-2250 Version 1.11.0.12. An authentication bypass vulnerability has been identified. The existing file system architecture could allow attackers to bypass the access control that may allow remote code execution.	2017-05-18	not yet calculated	CVE-2017-5174 BID MISC
geutebruck -- ip_camera	An Improper Neutralization of Special Elements (in an OS command) issue was discovered in Geutebruck IP Camera G-Cam/EFD-2250 Version 1.11.0.12. An improper neutralization of special elements vulnerability has been identified. If special elements are not properly neutralized, an attacker can call multiple parameters that can allow access to the root level operating system which could allow remote code execution.	2017-05-18	not yet calculated	CVE-2017-5173 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gnu -- binutils	GNU Binutils 2.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to MIPS GOT mishandling in the process_mips_specific function in readelf.c.	2017-05-17	not yet calculated	CVE-2017-9041 MISC MISC MISC
gnu -- binutils	GNU Binutils 2017-04-03 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash), related to the process_mips_specific function in readelf.c, via a crafted ELF file that triggers a large memory-allocation attempt.	2017-05-17	not yet calculated	CVE-2017-9040 MISC MISC
gnu -- binutils	readelf.c in GNU Binutils 2017-04-12 has a "cannot be represented in type long" issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file.	2017-05-17	not yet calculated	CVE-2017-9042 MISC MISC
gnu -- binutils	readelf.c in GNU Binutils 2017-04-12 has a "shift exponent too large for type unsigned long" issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file.	2017-05-17	not yet calculated	CVE-2017-9043 MISC MISC
gnu -- binutils	The print_symbol_for_build_attribute function in readelf.c in GNU Binutils 2017-04-12 allows remote attackers to cause a denial of service (invalid read and SEGV) via a crafted ELF file.	2017-05-17	not yet calculated	CVE-2017-9044 MISC
gnu -- binutils	GNU Binutils 2.28 allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file with many program headers, related to the get_program_headers function in readelf.c.	2017-05-17	not yet calculated	CVE-2017-9039 MISC MISC
gnu -- binutils	GNU Binutils 2.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to the byte_get_little_endian function in elfcomm.c, the get_unwind_section_word function in readelf.c, and ARM unwind information that contains invalid word offsets.	2017-05-17	not yet calculated	CVE-2017-9038 MISC MISC
google -- android	The Android Apps Money Forward (prior to v7.18.0), Money Forward for The Gunma Bank (prior to v1.2.0), Money Forward for SHIGA BANK (prior to v1.2.0), Money Forward for SHIZUOKA BANK (prior to v1.4.0), Money Forward for SBI Sumishin Net Bank (prior to v1.6.0), Money Forward for Tokai Tokyo Securities (prior to v1.4.0), Money Forward for THE TOHO BANK (prior to v1.3.0), Money Forward for YMFG (prior to v1.5.0) provided by Money Forward, Inc. and Money Forward for AppPass (prior to v7.18.3), Money Forward for au SMARTPASS (prior to v7.18.0), Money Forward for Chou Houdai (prior to v7.18.3) provided by SOURCENEXT CORPORATION do not properly implement the WebView class, which allows an attacker to disclose information stored on the device via a specially crafted application.	2017-05-12	not yet calculated	CVE-2016-4839 CONFIRM BID MISC JVN
google -- android	The Google I/O 2017 application before 5.1.4 for Android downloads multiple .json files from http://storage.googleapis.com without SSL, which makes it easier for man-in-the-middle attackers to spoof Feed and Schedule data by creating a modified blocks_v4.json file.	2017-05-18	not yet calculated	CVE-2017-9045 MISC
google -- android	** DISPUTED ** Facebook WhatsApp Messenger 2.17.146 for Android uses the SD card for cleartext storage of files (Audio, Documents, Images, Video, and Voice Notes) associated with a chat, even after that chat is deleted. There may be users who expect file deletion to occur upon chat deletion, or who expect encryption (consistent with the application's use of an encrypted database to store chat text). NOTE: the vendor reportedly indicates that they do not "consider these to be security issues" because a user may legitimately want to preserve any file for use "in other apps like the Google Photos gallery" regardless of whether its associated chat is deleted.	2017-05-18	not yet calculated	CVE-2017-8769 MISC
google -- android	In TrustZone, an integer overflow vulnerability can potentially occur in all Android releases from CAF using the Linux kernel due to an improper address range computation.	2017-05-16	not yet calculated	CVE-2014-9932 BID CONFIRM
google -- android	The Android Apps Money Forward (prior to v7.18.0), Money Forward for The Gunma Bank (prior to v1.2.0), Money Forward for SHIGA BANK (prior to v1.2.0), Money Forward for SHIZUOKA BANK (prior to v1.4.0), Money Forward for SBI Sumishin Net Bank (prior to v1.6.0), Money Forward for Tokai Tokyo Securities (prior to v1.4.0), Money Forward for THE TOHO BANK (prior to v1.3.0), Money Forward for YMFG (prior to v1.5.0) provided by Money Forward, Inc. and Money Forward for AppPass (prior to v7.18.3), Money Forward for au SMARTPASS (prior to v7.18.0), Money Forward for Chou Houdai (prior to v7.18.3) provided by SOURCENEXT CORPORATION allows an attacker to execute unintended operations via a specially crafted application.	2017-05-12	not yet calculated	CVE-2016-4838 CONFIRM BID MISC JVN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
halliburton -- logview_pro	Buffer overflow in Halliburton LogView Pro 10.0.1 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .tif file.	2017-05-15	not yet calculated	CVE-2017-8926 EXPLOIT-DB
hootoo_trip_mate -- heap_buffer	Stack buffer overflow in vshttpd (aka ioos) in HooToo Trip Mate 6 (TM6) firmware 2.000.030 and earlier allows remote unauthenticated attackers to control the program counter via a specially crafted fname parameter of a GET request.	2017-05-17	not yet calculated	CVE-2017-9026 MISC
hootoo_trip_mate-- heap_buffer	Heap buffer overflow in vshttpd (aka ioos) in HooToo Trip Mate 6 (TM6) firmware 2.000.030 and earlier allows remote unauthenticated attackers to control the program counter via a specially crafted HTTP Cookie header.	2017-05-17	not yet calculated	CVE-2017-9025 MISC
ibm -- distributed_marketing	IBM Distributed Marketing 8.6, 9.0, and 10.0 could allow a privileged authenticated user to create an instance that gets created with security profile not valid for the templates, that results in the new instance not accessible for the intended user. IBM X-Force ID: 116379.	2017-05-15	not yet calculated	CVE-2016-5979 CONFIRM
ibm -- jazz_foundation	IBM Jazz Foundation could allow an authenticated user to obtain sensitive information from stack traces. IBM X-Force ID: 119781,	2017-05-15	not yet calculated	CVE-2016-9735 CONFIRM
ibm -- qradar	IBM QRadar 7.2 and 7.3 stores user credentials in plain in clear text which can be read by an authenticated user. IBM X-Force ID: 120207.	2017-05-15	not yet calculated	CVE-2016-9750 CONFIRM
imagemagick -- rle_decoder	ImageMagick before 7.0.5-2 and GraphicsMagick before 1.3.24 use uninitialized memory in the RLE decoder, allowing an attacker to leak sensitive information from process memory space, as demonstrated by remote attacks against ImageMagick code in a long-running server process that converts image data on behalf of multiple users. This is caused by a missing initialization step in the ReadRLEImage function in coders/rle.c.	2017-05-19	not yet calculated	CVE-2017-9098 MISC MISC MISC
imagworsener -- libimageworsener.a	The lzw_add_to_dict function in imagew-gif.c in libimageworsener.a in ImageWorsener 1.3.1 allows remote attackers to cause a denial of service (infinite loop) via a crafted image.	2017-05-19	not yet calculated	CVE-2017-9094 CONFIRM
imagworsener -- libimageworsener.a	The my_skip_input_data_fn function in imagew-jpeg.c in libimageworsener.a in ImageWorsener 1.3.1 allows remote attackers to cause a denial of service (infinite loop) via a crafted image.	2017-05-19	not yet calculated	CVE-2017-9093 CONFIRM
infor -- eam	INFOR EAM V11.0 Build 201410 has XSS via comment fields.	2017-05-16	not yet calculated	CVE-2017-7953 MISC
infor -- eam	INFOR EAM V11.0 Build 201410 has SQL injection via search fields, related to the filtervalue parameter.	2017-05-16	not yet calculated	CVE-2017-7952 MISC
ios -- life_before_us_yo_app	The Life Before Us Yo app 2.5.8 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2017-05-15	not yet calculated	CVE-2017-8937 MISC
ios-- ellentube_app	The Warner Bros. ellentube app 3.1.1 through 3.1.3 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2017-05-15	not yet calculated	CVE-2017-8939 MISC
ios -- food_scanner_app	The YottaMark ShopWell - Healthy Diet & Grocery Food Scanner app 5.3.7 through 5.4.2 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2017-05-15	not yet calculated	CVE-2017-8942 MISC
ios -- grocery_deals_app	The Zipongo - Healthy Recipes and Grocery Deals app before 6.3 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2017-05-15	not yet calculated	CVE-2017-8940 MISC
ios -- international_app	The Interval International app 3.3 through 3.5.1 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2017-05-15	not yet calculated	CVE-2017-8941 MISC
ios -- pumatrac_app	The PUMA PUMATRAC app 3.0.2 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2017-05-15	not yet calculated	CVE-2017-8943 MISC
ios -- radio_javan	The Radio Javan app 9.3.4 through 9.6.1 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2017-05-15	not yet calculated	CVE-2017-8938 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ipswitch -- moveit_transfer	Ipswitch MOVEit Transfer (formerly DMZ) allows pre-authentication blind SQL injection. The fixed versions are MOVEit Transfer 2017 9.0.0.201, MOVEit DMZ 8.3.0.30, and MOVEit DMZ 8.2.0.20.	2017-05-18	not yet calculated	CVE-2017-6195 CONFIRM
jms-- jboss	HTTPServerILServlet.java in JMS over HTTP Invocation Layer of the JbossMQ implementation, which is enabled by default in Red Hat Jboss Application Server <= Jboss 4.X does not restrict the classes for which it performs deserialization, which allows remote attackers to execute arbitrary code via crafted serialized data.	2017-05-19	not yet calculated	CVE-2017-7504 CONFIRM
joomla -- b2j_contact	The Codextrous B2J Contact (aka b2j_contact) extension before 2.1.13 for Joomla! allows a directory traversal attack that bypasses a uniqid protection mechanism, and makes it easier to read arbitrary uploaded files.	2017-05-17	not yet calculated	CVE-2017-9030 MISC
joomla -- codextrous_b2j_contact	The Codextrous B2J Contact (aka b2j_contact) extension before 2.1.13 for Joomla! allows a rename attack that bypasses a "safe file extension" protection mechanism, leading to remote code execution.	2017-05-17	not yet calculated	CVE-2017-5215 MISC
joomla -- codextrous_b2j_contact	The Codextrous B2J Contact (aka b2j_contact) extension before 2.1.13 for Joomla! allows prediction of a uniqid value based on knowledge of a time value. This makes it easier to read arbitrary uploaded files.	2017-05-17	not yet calculated	CVE-2017-5214 MISC
joomla -- sql_injection	SQL injection vulnerability in Joomla! 3.7.x before 3.7.1 allows attackers to execute arbitrary SQL commands via unspecified vectors.	2017-05-17	not yet calculated	CVE-2017-8917 CONFIRM
kde -- kdelibs	KDE kdelibs before 4.14.32 and KAuth before 5.34 allow local users to gain root privileges by spoofing a callerID and leveraging a privileged helper app.	2017-05-17	not yet calculated	CVE-2017-8422 MLIST CONFIRM CONFIRM CONFIRM CONFIRM
larson -- vizex-reader	Buffer overflow in Larson VizEx Reader 9.7.5 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .tif file.	2017-05-15	not yet calculated	CVE-2017-8927 EXPLOIT-DB
lcds -- improper_access_control	An Improper Access Control issue was discovered in LCDS - Leao Consultoria e Desenvolvimento de Sistemas LTDA ME LAquis SCADA. The following versions are affected: Versions 4.1 and prior versions released before January 20, 2017. An Improper Access Control vulnerability has been identified, which may allow an authenticated user to modify application files to escalate privileges.	2017-05-18	not yet calculated	CVE-2017-6016 BID MISC
libav -- libavformat/nsvdec.c	libav before 12.1 is vulnerable to an invalid read of size 1 due to NULL pointer dereferencing in the nsv_read_chunk function in libavformat/nsvdec.c.	2017-05-18	not yet calculated	CVE-2017-9051 MISC MISC
libdwarf -- dw 201703-001	An issue, also known as DW201703-001, was discovered in libdwarf 2017-03-21. In dwarf_formsdata() a few data types were not checked for being in bounds, leading to a heap-based buffer over-read.	2017-05-18	not yet calculated	CVE-2017-9055 MISC
libdwarf -- dw 201703-002	An issue, also known as DW201703-002, was discovered in libdwarf 2017-03-21. In _dwarf_decode_s_leb128_chk() a byte pointer was dereferenced just before it was checked for being in bounds, leading to a heap-based buffer over-read.	2017-05-18	not yet calculated	CVE-2017-9054 MISC
libdwarf -- dw 201703-005	An issue, also known as DW201703-005, was discovered in libdwarf 2017-03-21. A heap-based buffer over-read in _dwarf_read_loc_expr_op() is due to a failure to check a pointer for being in bounds (in a few places in this function).	2017-05-18	not yet calculated	CVE-2017-9053 MISC
libdwarf -- dw 201703-006	An issue, also known as DW201703-006, was discovered in libdwarf 2017-03-21. A heap-based buffer over-read in dwarf_formsdata() is due to a failure to check a pointer for being in bounds (in a few places in this function) and a failure in a check in dwarf_attr_list().	2017-05-18	not yet calculated	CVE-2017-9052 MISC
libmenu -- cache	Libmenu-cache 1.0.2 insecurely uses /tmp for a socket file, allowing a local user to cause a denial of service (menu unavailability).	2017-05-15	not yet calculated	CVE-2017-8933 CONFIRM CONFIRM
libraw -- foveon_load_camf()	A boundary error within the "foveon_load_camf()" function (dcraw_foveon.c) when initializing a huffman table in LibRaw-demosaic-pack-GPL2 before 0.18.2 can be exploited to cause a stack-based buffer overflow.	2017-05-15	not yet calculated	CVE-2017-6890 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
libraw -- foveon_load_camf()	An integer overflow error within the "foveon_load_camf()" function (dcraw_foveon.c) in LibRaw-demosaic-pack-GPL2 before 0.18.2 can be exploited to cause a heap-based buffer overflow.	2017-05-15	not yet calculated	CVE-2017-6889 CONFIRM MISC
libraw -- parse_tiff_ifd()	A boundary error within the "parse_tiff_ifd()" function (internal/dcraw_common.cpp) in LibRaw versions before 0.18.2 can be exploited to cause a memory corruption via e.g. a specially crafted KDC file with model set to "DSLR-A100" and containing multiple sequences of 0x100 and 0x14A TAGs.	2017-05-16	not yet calculated	CVE-2017-6887 MISC MISC MISC
libraw -- parse_tiff_ifd()	An error within the "parse_tiff_ifd()" function (internal/dcraw_common.cpp) in LibRaw versions before 0.18.2 can be exploited to corrupt memory.	2017-05-16	not yet calculated	CVE-2017-6886 CONFIRM MISC MISC
libxml 2 -- 20904 -gitv 2.9.4-16 -g 0741801	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a heap-based buffer over-read in the xmlDictComputeFastKey function in dict.c. This vulnerability causes programs that use libxml2, such as PHP, to crash. This vulnerability exists because of an incomplete fix for libxml2 Bug 759398.	2017-05-18	not yet calculated	CVE-2017-9049 MISC
libxml 2 -- 20904 -gitv 2.9.4-16 -g 0741801	libxml 2 20904 -GITv 2.9.4-16 -g 0741801 is vulnerable to a heap-based buffer over-read in the xmlDictAddString function in dict.c. This vulnerability causes programs that use libxml2, such as PHP, to crash. This vulnerability exists because of an incomplete fix for CVE -2016-1839 .	2017-05-18	not yet calculated	CVE-2017-9050 MISC
libxml 2 -- 20904 -gitv 2.9.4-16 -g 0741801	libxml 2 20904 -GITv 2.9.4-16 -g 0741801 is vulnerable to a stack-based buffer overflow. The function xmlSnprintfElementContent in valid.c is supposed to recursively dump the element content definition into a char buffer 'buf' of size 'size'. At the end of the routine, the function may strcat two more characters without checking whether the current strlen(buf) + 2 < size. This vulnerability causes programs that use libxml2, such as PHP, to crash.	2017-05-18	not yet calculated	CVE-2017-9048 MISC
libxml 2 -- 20904 -gitv 2.9.4-16 -g 0741801	A buffer overflow was discovered in libxml 2 20904 -GITv 2.9.4-16 -g 0741801 . The function xmlSnprintfElementContent in valid.c is supposed to recursively dump the element content definition into a char buffer 'buf' of size 'size'. The variable len is assigned strlen(buf). If the content->type is XML_ELEMENT_CONTENT_ELEMENT, then (i) the content->prefix is appended to buf (if it actually fits) whereupon (ii) content->name is written to the buffer. However, the check for whether the content->name actually fits also uses 'len' rather than the updated buffer length strlen(buf). This allows us to write about "size" many bytes beyond the allocated memory. This vulnerability causes programs that use libxml2, such as PHP, to crash.	2017-05-18	not yet calculated	CVE-2017-9047 MISC
libytnef -- ytnef	In libytnef in ytnef through 1.9.2, there is a heap-based buffer over-read due to incorrect boundary checking in the SIZECHECK macro in lib/ytnef.c.	2017-05-18	not yet calculated	CVE-2017-9058 CONFIRM
linux -- kernel	fs/ext4/inode.c in the Linux kernel before 4.6.2, when ext4 data=ordered mode is used, mishandles a needs-flushing-before-commit list, which allows local users to obtain sensitive information from other users' files in opportunistic circumstances by waiting for a hardware reset, creating a new file, making write system calls, and reading this file.	2017-05-15	not yet calculated	CVE-2017-7495 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
linux -- kernel	If shared content protection memory were passed as the secure camera memory buffer by the HLOS to a trusted application (TA) in all Android releases from CAF using the Linux kernel, the TA would not detect an issue and it would be treated as secure memory.	2017-05-16	not yet calculated	CVE-2016-10237 BID CONFIRM
linux -- kernel	In TrustZone access control policy may potentially be bypassed in all Android releases from CAF using the Linux kernel due to improper input validation an integer overflow vulnerability leading to a buffer overflow could potentially occur and a buffer over-read vulnerability could potentially occur.	2017-05-16	not yet calculated	CVE-2016-10239 BID CONFIRM
linux -- kernel	In QSEE in all Android releases from CAF using the Linux kernel access control may potentially be bypassed due to a page alignment issue.	2017-05-16	not yet calculated	CVE-2016-10238 BID CONFIRM
linux -- kernel	The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE -2017-8890 .	2017-05-19	not yet calculated	CVE-2017-9075 CONFIRM CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- kernel	In TrustZone an untrusted pointer dereference vulnerability can potentially occur in a DRM routine in all Android releases from CAF using the Linux kernel.	2017-05-16	not yet calculated	CVE-2015-9000 BID CONFIRM
linux -- kernel	The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE -2017-8890 .	2017-05-19	not yet calculated	CVE-2017-9077 CONFIRM CONFIRM CONFIRM
linux -- kernel	The dccp_v6_request_recv_sock function in net/dccp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE -2017-8890 .	2017-05-19	not yet calculated	CVE-2017-9076 CONFIRM CONFIRM CONFIRM
linux -- kernel	In TrustZone an integer overflow vulnerability can potentially occur in all Android releases from CAF using the Linux kernel.	2017-05-16	not yet calculated	CVE-2015-8998 BID CONFIRM
linux -- kernel	In TrustZone an information exposure vulnerability can potentially occur in all Android releases from CAF using the Linux kernel.	2017-05-16	not yet calculated	CVE-2015-9001 BID CONFIRM
linux -- kernel	In TrustZone an out-of-range pointer offset vulnerability can potentially occur in a DRM routine in all Android releases from CAF using the Linux kernel.	2017-05-16	not yet calculated	CVE-2015-9002 BID CONFIRM
linux -- kernel	In TrustZone a cryptographic issue can potentially occur in all Android releases from CAF using the Linux kernel.	2017-05-16	not yet calculated	CVE-2015-9003 BID CONFIRM
linux -- kernel	In TrustZone an integer overflow vulnerability can potentially occur in all Android releases from CAF using the Linux kernel.	2017-05-16	not yet calculated	CVE-2015-8995 BID CONFIRM
linux -- kernel	The ipxitf_ioctl function in net/ipx/af_ipx.c in the Linux kernel through 4.11.1 mishandles reference counts, which allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a failed SIOCGIFADDR ioctl call for an IPX interface.	2017-05-14	not yet calculated	CVE-2017-7487 CONFIRM CONFIRM CONFIRM CONFIRM
linux -- kernel	The IPv6 fragmentation implementation in the Linux kernel through 4.11.1 does not consider that the nexthdr field may be associated with an invalid option, which allows local users to cause a denial of service (out-of-bounds read and BUG) or possibly have unspecified other impact via crafted socket and send system calls.	2017-05-19	not yet calculated	CVE-2017-9074 CONFIRM CONFIRM CONFIRM
linux -- kernel	A buffer overflow vulnerability in all Android releases from CAF using the Linux kernel can potentially occur if an OEM performs an app region size customization due to a hard-coded value.	2017-05-16	not yet calculated	CVE-2014-9931 BID CONFIRM
linux -- kernel	In TrustZone a time-of-check time-of-use race condition could potentially exist in an authentication routine in all Android releases from CAF using the Linux kernel.	2017-05-16	not yet calculated	CVE-2014-9936 BID CONFIRM
linux -- kernel	In TrustZone an integer overflow vulnerability leading to a buffer overflow could potentially occur in a DRM routine in all Android releases from CAF using the Linux kernel.	2017-05-16	not yet calculated	CVE-2014-9935 BID CONFIRM
linux -- kernel	A time-of-check time-of-use race condition could potentially exist in the secure file system in all Android releases from CAF using the Linux kernel.	2017-05-16	not yet calculated	CVE-2016-10242 CONFIRM
linux -- kernel	In TrustZone a buffer overflow vulnerability can potentially occur in a DRM routine in all Android releases from CAF using the Linux kernel.	2017-05-16	not yet calculated	CVE-2014-9937 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- kernel	In TrustZone a buffer overflow vulnerability can potentially occur in all Android releases from CAF using the Linux kernel while loading an ELF file.	2017-05-16	not yet calculated	CVE-2015-8999 BID CONFIRM
linux -- kernel	In TrustZone a time-of-check time-of-use race condition could potentially exist in a QFPROM routine in all Android releases from CAF using the Linux kernel.	2017-05-16	not yet calculated	CVE-2015-8996 BID CONFIRM
linux -- kernel	Due to missing input validation in all Android releases from CAF using the Linux kernel, HLOS can write to fuses for which it should not have access.	2017-05-16	not yet calculated	CVE-2014-9933 BID CONFIRM
linux -- kernel	The NFSv4 implementation in the Linux kernel through 4.11.1 allows local users to cause a denial of service (resource consumption) by leveraging improper channel callback shutdown when unmounting an NFSv4 filesystem, aka a "module reference and kernel daemon" leak.	2017-05-18	not yet calculated	CVE-2017-9059 CONFIRM CONFIRM CONFIRM CONFIRM
linux -- kernel	A PKCS#1 v1.5 signature verification routine in all Android releases from CAF using the Linux kernel may not check padding.	2017-05-16	not yet calculated	CVE-2014-9934 BID CONFIRM
linux -- kernel	In TrustZone a time-of-check time-of-use race condition could potentially exist in a listener routine in all Android releases from CAF using the Linux kernel.	2017-05-16	not yet calculated	CVE-2015-8997 BID CONFIRM
mailcow -- mailcow	mailcow 0.14, as used in "mailcow: dockerized" and other products, has CSRF.	2017-05-14	not yet calculated	CVE-2017-8928 CONFIRM
mcafee -- ndlp	Clickjacking vulnerability in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote authenticated users to inject arbitrary web script or HTML via HTTP response header.	2017-05-17	not yet calculated	CVE-2017-4015 CONFIRM
mcafee -- ndlp	Banner Disclosure in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote attackers to obtain product information via HTTP response header.	2017-05-17	not yet calculated	CVE-2017-4013 CONFIRM
mcafee -- ndlp	Session Side jacking vulnerability in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote authenticated users to view, add, and remove users via modification of the HTTP request.	2017-05-17	not yet calculated	CVE-2017-4014 CONFIRM
mcafee -- ndlp	Web Server method disclosure in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote attackers to exploit and find another hole via HTTP response header.	2017-05-17	not yet calculated	CVE-2017-4016 CONFIRM
mcafee -- ndlp	User Name Disclosure in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote attackers to view user information via the appliance web interface.	2017-05-17	not yet calculated	CVE-2017-4017 CONFIRM
mcafee -- ndlp	Privilege Escalation vulnerability in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote authenticated users to view confidential information via modification of the HTTP request.	2017-05-17	not yet calculated	CVE-2017-4012 CONFIRM
mcafee -- ndlp	Embedding Script (XSS) in HTTP Headers vulnerability in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote attackers to get session/cookie information via modification of the HTTP request.	2017-05-17	not yet calculated	CVE-2017-4011 CONFIRM
mcafee -- orchestrator	A directory traversal vulnerability in the ePO Extension in McAfee ePolicy Orchestrator (ePO) 5.9.0, 5.3.2, and 5.1.3 and earlier allows remote authenticated users to execute a command of their choice via an authenticated ePO session.	2017-05-18	not yet calculated	CVE-2017-3980 CONFIRM
microfocus -- vibe	An absolute path traversal vulnerability (CWE-36) in Micro Focus Vibe 4.0.2 and earlier allows a remote authenticated attacker to download arbitrary files from the server by submitting a specially crafted request to the viewFile endpoint. Note that the attack can be performed without authentication if Guest access is enabled (Guest access is disabled by default).	2017-05-18	not yet calculated	CVE-2017-7433 CONFIRM
microsoft-- explorer	A security feature bypass vulnerability exists in Internet Explorer that allows for bypassing Mixed Content warnings, aka "Internet Explorer Security Feature Bypass Vulnerability."	2017-05-12	not yet calculated	CVE-2017-0064 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- .net_framework	Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7 allow an attacker to bypass Enhanced Security Usage taggings when they present a certificate that is invalid for a specific use, aka ".NET Security Feature Bypass Vulnerability."	2017-05-12	not yet calculated	CVE-2017-0248 BID CONFIRM
microsoft -- activex	An information disclosure vulnerability exists in the way some ActiveX objects are instantiated, aka "Microsoft ActiveX Information Disclosure Vulnerability."	2017-05-12	not yet calculated	CVE-2017-0242 BID CONFIRM
microsoft -- browser	A remote code execution vulnerability exists in Microsoft browsers in the way JavaScript scripting engines handle objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE -2017-0224 , CVE -2017-0228 , CVE -2017-0229 , CVE -2017-0230 , CVE -2017-0234 , CVE -2017-0235 , and CVE -2017-0236 .	2017-05-12	not yet calculated	CVE-2017-0238 BID CONFIRM
microsoft -- browser	A spoofing vulnerability exists when Microsoft browsers render SmartScreen Filter, aka "Microsoft Browser Spoofing Vulnerability."	2017-05-12	not yet calculated	CVE-2017-0231 BID CONFIRM
microsoft -- browsers	A remote code execution vulnerability exists in Microsoft browsers in the way JavaScript engines render when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE -2017-0224 , CVE -2017-0229 , CVE -2017-0230 , CVE -2017-0234 , CVE -2017-0235 , CVE -2017-0236 , and CVE -2017-0238 .	2017-05-12	not yet calculated	CVE-2017-0228 BID CONFIRM
microsoft -- chakra_core	A remote code execution vulnerability exists in Microsoft Chakra Core in the way JavaScript engines render when handling objects in memory. aka "Scripting Engine Memory Corruption Vulnerability". This vulnerability is unique from CVE -2017-0252 .	2017-05-15	not yet calculated	CVE-2017-0223 CONFIRM
microsoft -- chakra_core	A remote code execution vulnerability exists in Microsoft Chakra Core in the way JavaScript engines render when handling objects in memory. aka "Scripting Engine Memory Corruption Vulnerability". This vulnerability is unique from CVE -2017-0223 .	2017-05-15	not yet calculated	CVE-2017-0252 CONFIRM
microsoft -- edge	A remote code execution vulnerability exists in Microsoft Edge in the way affected Microsoft scripting engines render when handling objects in memory, aka "Microsoft Edge Remote Code Execution Vulnerability."	2017-05-12	not yet calculated	CVE-2017-0266 BID CONFIRM
microsoft -- edge	A vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This CVE ID is unique from CVE -2017-0227 and CVE -2017-0240 .	2017-05-12	not yet calculated	CVE-2017-0221 BID CONFIRM
microsoft -- edge	A remote code execution vulnerability exists in the way JavaScript engines render when handling objects in memory in Microsoft Edge, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE -2017-0228 , CVE -2017-0229 , CVE -2017-0230 , CVE -2017-0234 , CVE -2017-0235 , CVE -2017-0236 , and CVE -2017-0238 .	2017-05-12	not yet calculated	CVE-2017-0224 BID CONFIRM
microsoft -- edge	A remote code execution vulnerability exists in Microsoft Edge in the way affected Microsoft scripting engines render when handling objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This CVE ID is unique from CVE -2017-0221 and CVE -2017-0240 .	2017-05-12	not yet calculated	CVE-2017-0227 BID CONFIRM
microsoft -- edge	A remote code execution vulnerability exists in Microsoft Edge in the way JavaScript engines render when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE -2017-0224 , CVE -2017-0228 , CVE -2017-0230 , CVE -2017-0234 , CVE -2017-0235 , CVE -2017-0236 , and CVE -2017-0238 .	2017-05-12	not yet calculated	CVE-2017-0229 BID CONFIRM
microsoft -- edge	A remote code execution vulnerability exists in Microsoft Edge in the way that the Chakra JavaScript engine renders when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE -2017-0224 , CVE -2017-0228 , CVE -2017-0229 , CVE -2017-0230 , CVE -2017-0235 , CVE -2017-0236 , and CVE -2017-0238 .	2017-05-12	not yet calculated	CVE-2017-0234 BID CONFIRM
microsoft -- edge	An elevation of privilege vulnerability exists in Microsoft Edge that could allow an attacker to escape from the AppContainer sandbox in the browser, aka "Microsoft Edge Elevation of Privilege Vulnerability." This CVE ID is unique from CVE -2017-0241 .	2017-05-12	not yet calculated	CVE-2017-0233 BID CONFIRM
microsoft -- edge	The kernel-mode drivers in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1 and Windows Server 2012 Gold allow a local authenticated attacker to execute a specially crafted application to obtain kernel information, aka "Win32k Information Disclosure Vulnerability."	2017-05-12	not yet calculated	CVE-2017-0245 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- edge	A remote code execution vulnerability exists in Microsoft Edge in the way that the Chakra JavaScript engine renders when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE -2017-0224 , CVE -2017-0228 , CVE -2017-0229 , CVE -2017-0230 , CVE -2017-0234 , CVE -2017-0235 , and CVE -2017-0238 .	2017-05-12	not yet calculated	CVE-2017-0236 BID CONFIRM
microsoft -- edge	An elevation of privilege vulnerability exists when Microsoft Edge renders a domain-less page in the URL, which could allow Microsoft Edge to perform actions in the context of the Intranet Zone and access functionality that is not typically available to the browser when browsing in the context of the Internet Zone, aka "Microsoft Edge Elevation of Privilege Vulnerability." This CVE ID is unique from CVE -2017-0233 .	2017-05-12	not yet calculated	CVE-2017-0241 BID CONFIRM
microsoft -- edge	A remote code execution vulnerability exists in Microsoft Edge in the way affected Microsoft scripting engines render when handling objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This CVE ID is unique from CVE -2017-0221 and CVE -2017-0227 .	2017-05-12	not yet calculated	CVE-2017-0240 BID CONFIRM
microsoft -- edge	A remote code execution vulnerability exists in Microsoft Edge in the way JavaScript engines render when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE -2017-0224 , CVE -2017-0228 , CVE -2017-0229 , CVE -2017-0234 , CVE -2017-0235 , CVE -2017-0236 , and CVE -2017-0238 .	2017-05-12	not yet calculated	CVE-2017-0230 BID CONFIRM
microsoft -- edge	A remote code execution vulnerability exists in Microsoft Edge in the way that the Chakra JavaScript engine renders when handling objects in memory, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE -2017-0224 , CVE -2017-0228 , CVE -2017-0229 , CVE -2017-0230 , CVE -2017-0234 , CVE -2017-0236 , and CVE -2017-0238 .	2017-05-12	not yet calculated	CVE-2017-0235 BID CONFIRM
microsoft -- explorer	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka "Internet Explorer Memory Corruption Vulnerability." This CVE ID is unique from CVE -2017-0222 .	2017-05-12	not yet calculated	CVE-2017-0226 BID CONFIRM
microsoft -- explorer	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka "Internet Explorer Memory Corruption Vulnerability." This CVE ID is unique from CVE -2017-0226 .	2017-05-12	not yet calculated	CVE-2017-0222 BID CONFIRM
microsoft -- office	Microsoft Office 2007 SP3, Office 2010 SP2, Office 2013 SP1, Office 2016, Office Online Server 2016, Office Web Apps 2010 SP2,Office Web Apps 2013 SP1, Project Server 2013 SP1, SharePoint Enterprise Server 2013 SP1, SharePoint Enterprise Server 2016, SharePoint Foundation 2013 SP1, Sharepoint Server 2010 SP2, Word 2016, and Skype for Business 2016 allow a remote code execution vulnerability when the software fails to properly handle objects in memory, aka "Office Remote Code Execution Vulnerability". This CVE ID is unique from CVE -2017-0261 and CVE -2017-0262 .	2017-05-12	not yet calculated	CVE-2017-0281 BID CONFIRM
microsoft -- office	Microsoft Office 2010 SP2, Office 2013 SP1, and Office 2016 allow a remote code execution vulnerability when the software fails to properly handle objects in memory, aka "Office Remote Code Execution Vulnerability". This CVE ID is unique from CVE -2017-0261 and CVE -2017-0281 .	2017-05-12	not yet calculated	CVE-2017-0262 BID CONFIRM
microsoft -- office	The kernel-mode drivers 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, 1703, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."	2017-05-12	not yet calculated	CVE-2017-0263 BID CONFIRM
microsoft -- office	Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Office Compatibility Pack SP3, Office for Mac 2011, Office for Mac 2016, Microsoft Office Web Apps 2010 SP2, Office Web Apps Server 2013 SP1, Word 2013 RT SP1, Word 2013 SP1, Word Automation Services on Microsoft SharePoint Server 2013 SP1, Office Word Viewer, SharePoint Enterprise Server 2016, and Word 2016 allow a remote code execution vulnerability when the software fails to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE -2017-0264 and CVE -2017-0265 .	2017-05-12	not yet calculated	CVE-2017-0254 BID CONFIRM
microsoft -- office	Microsoft Office 2010 SP2, Office 2013 SP1, and Office 2016 allow a remote code execution vulnerability when the software fails to properly handle objects in memory, aka "Office Remote Code Execution Vulnerability". This CVE ID is unique from CVE -2017-0262 and CVE -2017-0281 .	2017-05-12	not yet calculated	CVE-2017-0261 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- powerpoint	Microsoft PowerPoint for Mac 2011 allows a remote code execution vulnerability when the software fails to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE -2017-0254 and CVE -2017-0265 .	2017-05-12	not yet calculated	CVE-2017-0264 BID CONFIRM
microsoft -- powerpoint	Microsoft PowerPoint for Mac 2011 allows a remote code execution vulnerability when the software fails to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE -2017-0254 and CVE -2017-0264 .	2017-05-12	not yet calculated	CVE-2017-0265 BID CONFIRM
microsoft -- server	The Microsoft Server Message Block 1.0 (SMBv1) server on 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 attacker to execute remote code by the way it handles certain requests, aka "Windows SMB Remote Code Execution Vulnerability". This CVE ID is unique from CVE -2017-0272 , CVE -2017-0277 , and CVE -2017-0279 .	2017-05-12	not yet calculated	CVE-2017-0278 BID CONFIRM
microsoft -- server	The Graphics Component in the kernel-mode drivers 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, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application or in Windows 7 for x64-based Systems and later, cause denial of service, aka "Win32k Elevation of Privilege Vulnerability."	2017-05-12	not yet calculated	CVE-2017-0246 BID CONFIRM
microsoft -- server	The Windows kernel in Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows authenticated attackers to obtain sensitive information via a specially crafted document, aka "Windows Kernel Information Disclosure Vulnerability," a different vulnerability than CVE -2017-0175 , CVE -2017-0220 , and CVE -2017-0258 .	2017-05-12	not yet calculated	CVE-2017-0259 BID CONFIRM
microsoft -- server	The Microsoft Server Message Block 1.0 (SMBv1) allows denial of service when an attacker sends specially crafted requests to the server, aka "Windows SMB Denial of Service Vulnerability". This CVE ID is unique from CVE -2017-0269 and CVE -2017-0273 .	2017-05-12	not yet calculated	CVE-2017-0280 BID CONFIRM
microsoft -- server	The Microsoft Server Message Block 1.0 (SMBv1) server on 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 attacker to execute remote code by the way it handles certain requests, aka "Windows SMB Remote Code Execution Vulnerability". This CVE ID is unique from CVE -2017-0272 , CVE -2017-0277 , and CVE -2017-0278 .	2017-05-12	not yet calculated	CVE-2017-0279 BID CONFIRM
microsoft -- server	Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that 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 handles certain requests, aka "Windows SMB Information Disclosure Vulnerability". This CVE ID is unique from CVE -2017-0267 , CVE -2017-0268 , CVE -2017-0270 , CVE -2017-0271 , CVE -2017-0275 , and CVE -2017-0276 .	2017-05-12	not yet calculated	CVE-2017-0274 BID CONFIRM
microsoft -- server	Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that 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 handles certain requests, aka "Windows SMB Information Disclosure Vulnerability". This CVE ID is unique from CVE -2017-0267 , CVE -2017-0268 , CVE -2017-0271 , CVE -2017-0274 , CVE -2017-0275 , and CVE -2017-0276 .	2017-05-12	not yet calculated	CVE-2017-0270 BID CONFIRM
microsoft -- server	Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that 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 handles certain requests, aka "Windows SMB Information Disclosure Vulnerability". This CVE ID is unique from CVE -2017-0267 , CVE -2017-0268 , CVE -2017-0270 , CVE -2017-0274 , CVE -2017-0275 , and CVE -2017-0276 .	2017-05-12	not yet calculated	CVE-2017-0271 BID CONFIRM
microsoft -- server	The Microsoft Server Message Block 1.0 (SMBv1) allows denial of service when an attacker sends specially crafted requests to the server, aka "Windows SMB Denial of Service Vulnerability". This CVE ID is unique from CVE -2017-0273 and CVE -2017-0280 .	2017-05-12	not yet calculated	CVE-2017-0269 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- server	Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that 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 handles certain requests, aka "Windows SMB Information Disclosure Vulnerability". This CVE ID is unique from CVE -2017-0267 , CVE -2017-0270 , CVE -2017-0271 , CVE -2017-0274 , CVE -2017-0275 , and CVE -2017-0276 .	2017-05-12	not yet calculated	CVE-2017-0268 BID CONFIRM
microsoft -- server	Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that 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 handles certain requests, aka "Windows SMB Information Disclosure Vulnerability". This CVE ID is unique from CVE -2017-0268 , CVE -2017-0270 , CVE -2017-0271 , CVE -2017-0274 , CVE -2017-0275 , and CVE -2017-0276 .	2017-05-12	not yet calculated	CVE-2017-0267 BID CONFIRM
microsoft -- server	The kernel in Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows locally authenticated attackers to gain privileges via a crafted application, or in Windows 7 for x64-based systems, cause denial of service, aka "Windows Kernel Elevation of Privilege Vulnerability."	2017-05-12	not yet calculated	CVE-2017-0244 BID CONFIRM
microsoft -- server	The Microsoft Server Message Block 1.0 (SMBv1) server on 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 attacker to execute remote code by the way it handles certain requests, aka "Windows SMB Remote Code Execution Vulnerability". This CVE ID is unique from CVE -2017-0277 , CVE -2017-0278 , and CVE -2017-0279 .	2017-05-12	not yet calculated	CVE-2017-0272 BID CONFIRM
microsoft -- server	The Microsoft Server Message Block 1.0 (SMBv1) server on 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 attacker to execute remote code by the way it handles certain requests, aka "Windows SMB Remote Code Execution Vulnerability". This CVE ID is unique from CVE -2017-0272 , CVE -2017-0278 , and CVE -2017-0279 .	2017-05-12	not yet calculated	CVE-2017-0277 BID CONFIRM
microsoft -- server	Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that 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 handles certain requests, aka "Windows SMB Information Disclosure Vulnerability". This CVE ID is unique from CVE -2017-0267 , CVE -2017-0268 , CVE -2017-0270 , CVE -2017-0271 , CVE -2017-0274 , and CVE -2017-0275 .	2017-05-12	not yet calculated	CVE-2017-0276 BID CONFIRM
microsoft -- server	Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that 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 handles certain requests, aka "Windows SMB Information Disclosure Vulnerability". This CVE ID is unique from CVE -2017-0267 , CVE -2017-0268 , CVE -2017-0270 , CVE -2017-0271 , CVE -2017-0274 , and CVE -2017-0276 .	2017-05-12	not yet calculated	CVE-2017-0275 BID CONFIRM
microsoft -- server	The Microsoft Server Message Block 1.0 (SMBv1) allows denial of service when an attacker sends specially crafted requests to the server, aka "Windows SMB Denial of Service Vulnerability". This CVE ID is unique from CVE -2017-0269 and CVE -2017-0280 .	2017-05-12	not yet calculated	CVE-2017-0273 BID CONFIRM
microsoft -- server	The 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, 1703, and Windows Server 2016 allows authenticated attackers to obtain sensitive information via a specially crafted document, aka "Windows Kernel Information Disclosure Vulnerability," a different vulnerability than CVE -2017-0175 , CVE -2017-0220 , and CVE -2017-0259 .	2017-05-12	not yet calculated	CVE-2017-0258 BID CONFIRM
microsoft -- sharepoint_foundation	Microsoft SharePoint Foundation 2013 SP1 allows an elevation of privilege vulnerability when it does not properly sanitize a specially crafted web request, aka "Microsoft SharePoint XSS Vulnerability".	2017-05-12	not yet calculated	CVE-2017-0255 BID CONFIRM
microsoft -- windows	The Windows kernel in Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows authenticated attackers to obtain sensitive information via a specially crafted document, aka "Windows Kernel Information Disclosure Vulnerability," a different vulnerability than CVE -2017-0220 , CVE -2017-0258 , and CVE -2017-0259 .	2017-05-12	not yet calculated	CVE-2017-0175 BID CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows	Windows COM Aggregate Marshaler 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 privilege vulnerability when an attacker runs a specially crafted application, aka "Windows COM Elevation of Privilege Vulnerability". This CVE ID is unique from CVE -2017-0214 .	2017-05-12	not yet calculated	CVE-2017-0213 BID CONFIRM
microsoft -- windows	Windows COM 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 privilege vulnerability when Windows fails to properly validate input before loading type libraries, aka "Windows COM Elevation of Privilege Vulnerability". This CVE ID is unique from CVE -2017-0213 .	2017-05-12	not yet calculated	CVE-2017-0214 BID CONFIRM
microsoft -- windows	The Windows kernel in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, and Windows Server 2012 Gold allows authenticated attackers to obtain sensitive information via a specially crafted document, aka "Windows Kernel Information Disclosure Vulnerability," a different vulnerability than CVE -2017-0175 , CVE -2017-0258 , and CVE -2017-0259 .	2017-05-12	not yet calculated	CVE-2017-0220 BID CONFIRM
microsoft -- windows	The GDI component 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 Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "GDI Information Disclosure Vulnerability."	2017-05-12	not yet calculated	CVE-2017-0190 BID CONFIRM
microsoft -- windows	Windows Hyper-V allows an elevation of privilege vulnerability when Microsoft Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 fail to properly validate vSMB packet data, aka "Windows Hyper-V vSMB Elevation of Privilege Vulnerability".	2017-05-12	not yet calculated	CVE-2017-0212 BID CONFIRM
microsoft -- windows	Windows DNS Server allows a denial of service vulnerability when Microsoft Windows Server 2008 SP2 and R2 SP1, Windows Server 2012 Gold and R2, and Windows Server 2016 are configured to answer version queries, aka "Windows DNS Server Denial of Service Vulnerability".	2017-05-12	not yet calculated	CVE-2017-0171 BID CONFIRM
microsoft -- windows	The kernel-mode drivers 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 allow a local authenticated attacker to execute a specially crafted application to obtain information, or in Windows 7 and later, cause denial of service, aka "Win32k Information Disclosure Vulnerability."	2017-05-12	not yet calculated	CVE-2017-0077 BID CONFIRM
microsoft -- windows	A buffer overflow in Smart Card authentication code in gpkcsp.dll in Microsoft Windows XP through SP3 and Server 2003 through SP2 allows a remote attacker to execute arbitrary code on the target computer, provided that the computer is joined in a Windows domain and has Remote Desktop Protocol connectivity (or Terminal Services) enabled.	2017-05-18	not yet calculated	CVE-2017-9073 MISC MISC
mikrotik -- l2tp	A vulnerability in MikroTik Version 6.38.5 could allow an unauthenticated remote attacker to exhaust all available CPU via a flood of UDP packets on port 500 (used for L2TP over IPsec), preventing the affected router from accepting new connections; all devices will be disconnected from the router and all logs removed automatically.	2017-05-18	not yet calculated	CVE-2017-8338 MISC MISC MISC MISC
mobotap_dolphin -- web_browser	The MoboTap Dolphin Web Browser - Fast Private Internet Search app 9.23.0 through 9.23.2 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2017-05-15	not yet calculated	CVE-2017-8936 MISC
modx-- revolution	In MODX Revolution before 2.5.7, an attacker is able to trigger Reflected XSS by injecting payloads into several fields on the setup page, as demonstrated by the database_type parameter.	2017-05-18	not yet calculated	CVE-2017-9068 MISC MISC
modx-- revolution	In MODX Revolution before 2.5.7, a user with file upload permissions is able to execute arbitrary code by uploading a file with the name .htaccess.	2017-05-18	not yet calculated	CVE-2017-9069 MISC MISC
modx-- revolution	In MODX Revolution before 2.5.7, a user with resource edit permissions can inject an XSS payload into the title of any post via the pagetitle parameter to connectors/index.php.	2017-05-18	not yet calculated	CVE-2017-9070 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
modx-- revolution	In MODX Revolution before 2.5.7, an attacker might be able to trigger XSS by injecting a payload into the HTTP Host header of a request. This is exploitable only in conjunction with other issues such as Cache Poisoning.	2017-05-18	not yet calculated	CVE-2017-9071 MISC MISC
modx-- revolution	In MODX Revolution before 2.5.7, when PHP 5.3.3 is used, an attacker is able to include and execute arbitrary files on the web server due to insufficient validation of the action parameter to setup/index.php, aka directory traversal.	2017-05-18	not yet calculated	CVE-2017-9067 MISC MISC MISC
moodle -- moodle	In Moodle 2.x and 3.x, searching of arbitrary blogs is possible because a capability check is missing.	2017-05-15	not yet calculated	CVE-2017-7490 CONFIRM
moodle -- moodle	In Moodle 2.x and 3.x, remote authenticated users can take ownership of arbitrary blogs by editing an external blog link.	2017-05-15	not yet calculated	CVE-2017-7489 CONFIRM
moodle -- moodle	In Moodle 2.x and 3.x, a CSRF attack is possible that allows attackers to change the "number of courses displayed in the course overview block" configuration setting.	2017-05-15	not yet calculated	CVE-2017-7491 CONFIRM
openvpn -- openvpn	OpenVPN versions before 2.3.15 and before 2.4.2 are vulnerable to reachable assertion when packet-ID counter rolls over resulting into Denial of Service of server by authenticated attacker.	2017-05-15	not yet calculated	CVE-2017-7479 CONFIRM
openvpn -- openvpn	OpenVPN version 2.3.12 and newer is vulnerable to unauthenticated Denial of Service of server via received large control packet. Note that this issue is fixed in 2.3.15 and 2.4.2.	2017-05-15	not yet calculated	CVE-2017-7478 CONFIRM
pcmanfm -- pcmanfm	PCManFM 1.2.5 insecurely uses /tmp for a socket file, allowing a local user to cause a denial of service (application unavailability).	2017-05-15	not yet calculated	CVE-2017-8934 CONFIRM CONFIRM
perlcritic -- perltidy	perltidy through 20160302 , as used by perlcritic, check-all-the-things, and other software, relies on the current working directory for certain output files and does not have a symlink-attack protection mechanism, which allows local users to overwrite arbitrary files by creating a symlink, as demonstrated by creating a perltidy.ERR symlink that the victim cannot delete.	2017-05-17	not yet calculated	CVE-2016-10374 CONFIRM
phoenix_contrac -- gmbh_mguard	An Improper Authentication issue was discovered in Phoenix Contact GmbH mGuard firmware versions 8.3.0 to 8.4.2. An attacker may be able to gain unauthorized access to the user firewall when RADIUS servers are unreachable.	2017-05-18	not yet calculated	CVE-2017-7937 MISC
phoenix_contrac -- gmbh_mguard	A Resource Exhaustion issue was discovered in Phoenix Contact GmbH mGuard firmware versions 8.3.0 to 8.4.2. An attacker may compromise the device's availability by performing multiple initial VPN requests.	2017-05-18	not yet calculated	CVE-2017-7935 MISC
phpwhois -- phpwhois	Cross-site scripting (XSS) vulnerability in phpwhois 4.2.5, as used in the adsense-click-fraud-monitoring plugin 1.7.5 for WordPress, allows remote attackers to inject arbitrary web script or HTML via the query parameter to whois.php.	2017-05-17	not yet calculated	CVE-2015-3998 MISC
playsms -- playsms	PlaySMS 1.4 allows remote code execution because PHP code in the name of an uploaded .php file is executed. sendfromfile.php has a combination of Unrestricted File Upload and Code Injection.	2017-05-19	not yet calculated	CVE-2017-9080 MISC EXPLOIT-DB
poppler -- evince	poppler 0.54.0, as used in Evince and other products, has a NULL pointer dereference in the JPXStream::readUByte function in JPXStream.cc. For example, the perf_test utility will crash (segmentation fault) when parsing an invalid PDF file.	2017-05-19	not yet calculated	CVE-2017-9083 MISC
qemu -- virtfs	Quick Emulator (Qemu) built with the VirtFS, host directory sharing via Plan 9 File System(9pfs) support, is vulnerable to an improper access control issue. It could occur while accessing virtfs metadata files in mapped-file security mode. A guest user could use this flaw to escalate their privileges inside guest.	2017-05-17	not yet calculated	CVE-2017-7493 MLIST CONFIRM MLIST
quest -- information_system	The Quest Information Systems Indiana Voters app 1.1.24 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2017-05-15	not yet calculated	CVE-2017-8935 MISC
redhat -- jboss	It was found that the Red Hat JBoss EAP 7.0.5 implementation of javax.xml.transform.TransformerFactory is vulnerable to XXE. An attacker could use this flaw to launch DoS or SSRF attacks, or read files from the server where EAP is deployed.	2017-05-18	not yet calculated	CVE-2017-7503 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rockwell -- automation_connected_workbench	A DLL Hijack issue was discovered in Rockwell Automation Connected Components Workbench (CCW). The following versions are affected: Connected Components Workbench - Developer Edition, v9.01.00 and earlier: 9328-CCWDEVENE, 9328-CCWDEVZHE, 9328-CCWDEVFRE, 9328-CCWDEVITE, 9328-CCWDEVDEE, 9328-CCWDEVESE, and 9328-CCWDEVPTE; and Connected Components Workbench - Free Standard Edition (All Supported Languages), v9.01.00 and earlier. Certain DLLs included with versions of CCW software can be potentially hijacked to allow an attacker to gain rights to a victim's affected personal computer. Such access rights can be at the same or potentially higher level of privileges as the compromised user account, including and up to computer administrator privileges.	2017-05-18	not yet calculated	CVE-2017-5176 BID MISC
schneider -- electric_wonderware_historian_client	An Improper XML Parser Configuration issue was discovered in Schneider Electric Wonderware Historian Client 2014 R2 SP1 and prior. An improperly restricted XML parser (with improper restriction of XML external entity reference, or XXE) may allow an attacker to enter malicious input through the application which could cause a denial of service or disclose file contents from a server or connected network.	2017-05-18	not yet calculated	CVE-2017-7907 MISC BID MISC
schneider -- electric_wonderware_indusoft_web	An Incorrect Default Permissions issue was discovered in Schneider Electric Wonderware InduSoft Web Studio v8.0 Patch 3 and prior versions. Upon installation, Wonderware InduSoft Web Studio creates a new directory and two files, which are placed in the system's path and can be manipulated by non-administrators. This could allow an authenticated user to escalate his or her privileges.	2017-05-19	not yet calculated	CVE-2017-7968 MISC MISC
sennet -- command_injection	A Command Injection issue was discovered in Satel Iberia SenNet Data Logger and Electricity Meters: SenNet Optimal DataLogger V5.37c-1.43c and prior, SenNet Solar Datalogger V5.03-1.56a and prior, and SenNet Multitask Meter V5.21a-1.18b and prior. Successful exploitation of this vulnerability could result in the attacker breaking out of the jailed shell and gaining full access to the system.	2017-05-18	not yet calculated	CVE-2017-6048 MISC
simple_invoices -- csrf	Multiple cross-site request forgery (CSRF) vulnerabilities in Simple Invoices 2013.1.beta.8 allow remote attackers to hijack the authentication of admins for requests that can (1) create new administrator user accounts and take over the entire application, (2) create regular user accounts, or (3) change configuration parameters such as tax rates and the enable/disable status of PayPal payment modules.	2017-05-14	not yet calculated	CVE-2017-8930 MISC
smb4k -- smb4k	smb4k before 2.0.1 allows local users to gain root privileges by leveraging failure to verify arguments to the mount helper DBUS service.	2017-05-17	not yet calculated	CVE-2017-8849 MLIST CONFIRM CONFIRM CONFIRM CONFIRM
vipa -- controls_winplc7	A Stack Buffer Overflow issue was discovered in VIPA Controls WinPLC7 5.0.45.5921 and prior. A stack-based buffer overflow vulnerability has been identified, where an attacker with a specially crafted packet could overflow the fixed length buffer. This could allow remote code execution.	2017-05-18	not yet calculated	CVE-2017-5177 BID MISC
wordpress -- filesystem_credentials_dialog	In WordPress before 4.7.5, a Cross Site Request Forgery (CSRF) vulnerability exists in the filesystem credentials dialog because a nonce is not required for updating credentials.	2017-05-18	not yet calculated	CVE-2017-9064 CONFIRM CONFIRM CONFIRM
wordpress -- http_class	In WordPress before 4.7.5, there is insufficient redirect validation in the HTTP class, leading to SSRF.	2017-05-18	not yet calculated	CVE-2017-9066 CONFIRM CONFIRM MISC CONFIRM
wordpress -- wordpress	In WordPress before 4.7.5, a cross-site scripting (XSS) vulnerability related to the Customizer exists, involving an invalid customization session.	2017-05-18	not yet calculated	CVE-2017-9063 CONFIRM CONFIRM CONFIRM
wordpress -- wordpress	In WordPress before 4.7.5, a cross-site scripting (XSS) vulnerability exists when attempting to upload very large files, because the error message does not properly restrict presentation of the filename.	2017-05-18	not yet calculated	CVE-2017-9061 CONFIRM CONFIRM CONFIRM
wordpress -- xml-rpc api	In WordPress before 4.7.5, there is a lack of capability checks for post meta data in the XML-RPC API.	2017-05-18	not yet calculated	CVE-2017-9065 CONFIRM CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- xml-rpc api	In WordPress before 4.7.5, there is improper handling of post meta data values in the XML-RPC API.	2017-05-18	not yet calculated	CVE-2017-9062 CONFIRM CONFIRM CONFIRM
wow -- moodboard	Open redirect vulnerability in the proxyimages function in wowproxy.php in the Wow Moodboard Lite plugin 1.1.1.1 for WordPress allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the url parameter.	2017-05-17	not yet calculated	CVE-2015-4070 BID MISC
yara -- libyara/sizedstr.c	The sized_string_cmp function in libyara/sizedstr.c in YARA 3.5.0 allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted rule.	2017-05-14	not yet calculated	CVE-2017-8929 CONFIRM CONFIRM
zimbra -- collaboration	Multiple cross-site request forgery (CSRF) vulnerabilities in the Admin Console in Zimbra Collaboration before 8.6.0 Patch 8 allow remote attackers to hijack the authentication of administrators for requests that (1) add, (2) modify, or (3) remove accounts by leveraging failure to use of a CSRF token and perform referer header checks, aka bugs 100885 and 100899.	2017-05-17	not yet calculated	CVE-2016-3403 FULLDISC BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
zoho -- manageengine_desktop	Zoho ManageEngine Desktop Central before build 100082 allows remote attackers to obtain control over all connected active desktops via unspecified vectors.	2017-05-15	not yet calculated	CVE-2017-7213 CONFIRM

ack to top