SB19-154
VULNERABILITY SUMMARY FOR MAY 2019

CYBERNETIC
GLOBAL INTELLIGENCE
Run Your Business. We'll Protect It.

SB19-154
Vulnerability Summary for May 2019

Cybernetic GI 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 Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. 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 determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by 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 10.0 - 7.0.

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 3.9 - 0.0

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

Source references taken from US-CERT.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7018 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7019 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7020 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7025 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7026 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7029 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7031 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7037 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7039 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7040 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	9.3	CVE-2019-7042 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	9.3	CVE-2019-7043 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	9.3	CVE-2019-7043 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	9.3	CVE-2019-7044 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	10.0	CVE-2019-7046 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	9.3	CVE-2019-7048 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7050 CONFIRM

adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code dexecution .	2019-05-24	10.0	CVE-2019-7051 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7052 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	10.0	CVE-2019-7054 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7060 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	10.0	CVE-2019-7062 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	10.0	CVE-2019-7066 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7068 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	9.3	CVE-2019-7069 CONFIRM MISC
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	9.3	CVE-2019-7070 CONFIRM MISC
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	9.3	CVE-2019-7072 CONFIRM MISC
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	7.1	CVE-2019-7075 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	10.0	CVE-2019-7076 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	9.3	CVE-2019-7077 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	9.3	CVE-2019-7078 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	9.3	CVE-2019-7079 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a double free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	10.0	CVE-2019-7080 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	10.0	CVE-2019-7082 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	10.0	CVE-2019-7083 CONFIRM

adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7084 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-05-24	10.0	CVE-2019-7085 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7086 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7087 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a data leakage (sensitive) vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	7.8	CVE-2019-7089 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20091 and earlier, 2019.010.20091 and earlier, 2017.011.30120 and earlier version, and 2015.006.30475 and earlier have a data leakage (sensitive) vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	7.8	CVE-2019-7815 CONFIRM
adobe -- coldfusion	ColdFusion versions Update 1 and earlier, Update 7 and earlier, and Update 15 and earlier have a deserialization of untrusted data vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7091 CONFIRM
adobe -- coldfusion	ColdFusion versions Update 2 and earlier, Update 9 and earlier, and Update 17 and earlier have a file upload restriction bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7816 CONFIRM
adobe -- digital_editions	Adobe Digital Editions versions 4.5.10.185749 and below have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7095 CONFIRM
adobe -- photoshop_cc	Adobe Photoshop CC 19.1.7 and earlier, and 20.0.2 and earlier have a heap corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-05-24	10.0	CVE-2019-7094 CONFIRM
apache -- hadoop	In Apache Hadoop versions 3.0.0-alpha1 to 3.1.0, 2.9.0 to 2.9.1, and 2.2.0 to 2.8.4, a user who can escalate to yarn user can possibly run arbitrary commands as root user.	2019-05-30	9.0	CVE-2018-8029 BID CONFIRM MLIST
auerswald -- comfortel_1200_ip_firmware	A command injection (missing input validation, escaping) in the ftp upgrade configuration interface on the Auerswald COMfort 1200 IP phone 3.4.4.1-10589 allows an authenticated remote attacker (simple user) -- in the same network as the device -- to trigger OS commands (like starting telnetd or opening a reverse shell) via a POST request to the web server.	2019-05-29	7.7	CVE-2018-19977 MISC MISC
auerswald -- comfortel_1200_ip_firmware	A buffer overflow vulnerability in the DHCP and PPPOE configuration interface of the Auerswald COMfort 1200 IP phone 3.4.4.1-10589 allows a remote attacker (authenticated as simple user in the same network as the device) to trigger remote code execution via a POST request (ManufacturerName parameter) to the web server on the device. The web server is running with root privileges and the injected code will also run with root privileges.	2019-05-29	7.7	CVE-2018-19978 MISC MISC
bosch -- bosch_video_management_system	A recently discovered security vulnerability affects all Bosch Video Management System (BVMS) versions 9.0 and below, DIVAR IP 2000, 3000, 5000 and 7000, Video Recording Manager (VRM), Video Streaming Gateway (VSG), Configuration Manager, Building Integration System (BIS) with Video Engine, Access Professional Edition (APE), Access Easy Controller (AEC), Bosch Video Client (BVC) and Video SDK (VSDK). The vulnerability potentially allows the unauthorized execution of code in the system via the network interface.	2019-05-29	7.5	CVE-2019-6957 CONFIRM
deltek -- maconomy	Deltek Maconomy 2.2.5 is prone to local file inclusion via absolute path traversal in the WS.macx1.W_MCS/ PATH_INFO, as demonstrated by a cgi-bin/Maconomy/MaconomyWS.macx1.W_MCS//etc/passwd URI.	2019-05-24	7.5	CVE-2019-12314 MISC MISC
exponentcms -- exponent_cms	Exponent CMS version 2.3.9 suffers from a sql injection vulnerability in framework/modules/ecommerce/controllers/cartController.php.	2019-05-24	7.5	CVE-2016-8898 MISC MISC
exponentcms -- exponent_cms	Exponent CMS version 2.3.9 suffers from a Object Injection vulnerability in framework/modules/core/controllers/expTagController.php related to change_tags.	2019-05-24	7.5	CVE-2016-8900 MISC MISC
firejail_project -- firejail	Firejail before 0.9.60 allows truncation (resizing to length 0) of the firejail binary on the host by running exploit code inside a firejail sandbox and having the sandbox terminated. To succeed, certain conditions need to be fulfilled: The jail (with the exploit code inside) needs to be started as root, and it also needs to be terminated as root from the host (either by stopping it ungracefully (e.g., SIGKILL), or by using the --shutdown control command). This is similar to CVE-2019-5736.	2019-05-31	9.3	CVE-2019-12499 MISC

fortinet -- forticlient	An Unsafe Search Path vulnerability in FortiClient Online Installer (Windows version before 6.0.6) may allow an unauthenticated, remote attacker with control over the directory in which FortiClientOnlineInstaller.exe resides to execute arbitrary code on the system via uploading malicious .dll files in that directory.	2019-05-28	9.3	CVE-2019-5589 CONFIRM
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Uncontrolled Resource Consumption (issue 2 of 2).	2019-05-29	7.8	CVE-2019-9177 MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 1 of 5).	2019-05-29	7.5	CVE-2019-9218 MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Insecure Permissions.	2019-05-29	7.5	CVE-2019-9485 MISC MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition 10.x (starting from 10.8) and 11.x before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control.	2019-05-29	7.5	CVE-2019-9732 MISC MISC
gitlab -- gitlab	file_copy_fallback in gio/gfile.c in GNOME GLib 2.15.0 through 2.61.1 does not properly restrict file permissions while a copy operation is in progress. Instead, default permissions are used.	2019-05-29	7.5	CVE-2019-12450 MISC
gnome -- gvfs	An issue was discovered in GNOME gvfs 1.29.4 through 1.41.2. daemon/gvfsbackendadmin.c mishandles file ownership because setfsuid is not used.	2019-05-29	7.5	CVE-2019-12447 MISC
gnome -- gvfs	An issue was discovered in GNOME gvfs 1.29.4 through 1.41.2. daemon/gvfsbackendadmin.c mishandles a file's user and group ownership during move (and copy with G_FILE_COPY_ALL_METADATA) operations from admin:// to file:// URIs, because root privileges are unavailable.	2019-05-29	10.0	CVE-2019-12449 MISC
gog -- galaxy	An exploitable local privilege elevation vulnerability exists in the file system permissions of the `Temp` directory in GOG Galaxy 1.2.48.36 (Windows 64-bit Installer). An attacker can overwrite executables of the Desktop Galaxy Updater to exploit this vulnerability and execute arbitrary code with SYSTEM privileges.	2019-05-30	7.2	CVE-2018-4048 MISC
karamasoft -- ultimateeditor	Karamasoft UltimateEditor 1 does not ensure that an uploaded file is an image or document (neither file types nor extensions are restricted). The attacker must use the Attach icon to perform an upload. An uploaded file is accessible under the UltimateEditorInclude/UserFiles/URI.	2019-05-24	7.5	CVE-2019-12150 MISC MISC
linux -- linux_kernel	An issue was discovered in wcd9335_codec_enable_dec in sound/soc/codecs/wcd9335.c in the Linux kernel through 5.1.5. It uses kstrndup instead of kmemdup_nul, which allows attackers to have an unspecified impact via unknown vectors.	2019-05-30	7.2	CVE-2019-12454 MISC MISC
linux -- linux_kernel	An issue was discovered in the MPT3COMMAND case in _ctl_ioctl_main in drivers/scsi/mpt3sas/mpt3sas_ctl.c in the Linux kernel through 5.1.5. It allows local users to cause a denial of service or possibly have unspecified other impact by changing the value of ioc_number between two kernel reads of that value, aka a "double fetch" vulnerability.	2019-05-30	7.2	CVE-2019-12456 MISC MISC
mlmsoftwarez -- add_clicking_mlm_software	SQL injection exists in ADD Clicking MLM Software 1.0, Binary MLM Software 1.0, Level MLM Software 1.0, Singleleg MLM Software 1.0, Autopool MLM Software 1.0, Investment MLM Software 1.0, Bidding MLM Software 1.0, Moneyorder MLM Software 1.0, Repurchase MLM Software 1.0, and Gift MLM Software 1.0 via the member/readmsg.php msg_id parameter, the member/tree.php pid parameter, or the member/downline.php m_id parameter.	2019-05-24	7.5	CVE-2018-17843 MISC MISC
mobotix -- s14_firmware	There is a lack of CSRF countermeasures on MOBOTIX S14 MX-V4.2.1.61 cameras, as demonstrated by adding an admin account via the /admin/access URI.	2019-05-31	9.3	CVE-2019-12502 MISC
precurio -- precurio	The Xinha plugin in Precurio 2.1 allows Directory Traversal, with resultant arbitrary code execution, via ExtendedFileManager/Classes/ExtendedFileManager.php because ExtendedFileManager can be used to rename the .htaccess file that blocks .php uploads.	2019-05-24	7.5	CVE-2016-10759 MISC MISC
qualcomm -- ipq4019_firmware	Data length received from firmware is not validated against the max allowed size which can result in buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24	2019-05-24	7.2	CVE-2018-11925 CONFIRM
qualcomm -- ipq4019_firmware	Improper check before assigning value can lead to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA4020, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9558, QCA9563, QCA9880, QCA9886, QCA9980, QCN5502, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SM7150, Snapdragon_High_Med_2016, SXR1130	2019-05-24	7.2	CVE-2018-11968 CONFIRM

qualcomm -- ipq8074_firmware	Lack of check on length parameter may cause buffer overflow while processing WMI commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9886, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SM7150, SXR1130	2019-05-24	7.2	CVE-2018-11928 CONFIRM
qualcomm -- mdm9150_firmware	Improper input validation on input which is used as an array index will lead to an out of bounds issue while processing AP find event from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 625, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24, SM7150	2019-05-24	7.2	CVE-2018-11927 CONFIRM
qualcomm -- mdm9150_firmware	Improper input validation on input data which is used to locate and copy the additional IEs in WLAN function can lead to potential integer truncation issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 675, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, SM7150	2019-05-24	10.0	CVE-2018-11930 CONFIRM
qualcomm -- mdm9150_firmware	Lack of input validation before copying can lead to a buffer over read in WLAN function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6574AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SM7150	2019-05-24	10.0	CVE-2018-11937 CONFIRM
qualcomm -- mdm9150_firmware	Lack of check in length before using memcpy in WLAN function can lead to OOB access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCS605, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130	2019-05-24	10.0	CVE-2018-11940 CONFIRM
qualcomm -- mdm9150_firmware	Failure to initialize the extra buffer can lead to an out of buffer access in WLAN function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24	2019-05-24	10.0	CVE-2018-11949 CONFIRM
qualcomm -- mdm9150_firmware	While processing ssid IE length from remote AP, possible out-of-bounds access may occur due to crafted ssid IE length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 650/52, SD 820, SD 820A, SDM439, SDX20	2019-05-24	10.0	CVE-2018-11953 CONFIRM
qualcomm -- mdm9150_firmware	Signature verification of the skel library could potentially be disabled as the memory region on the remote subsystem in which the library is loaded is allocated from userspace currently in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	2019-05-24	7.2	CVE-2018-11967 CONFIRM
qualcomm -- mdm9150_firmware	Unchecked OTA field in GNSS XTRA3 lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016, SXR1130	2019-05-24	10.0	CVE-2018-13886 CONFIRM

qualcomm -- mdm9150_firmware	Untrusted header fields in GNSS XTRA3 function can lead to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9650, MDM9655, MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, SXR1130	2019-05-24	10.0	CVE-2018-13887 CONFIRM
qualcomm -- mdm9150_firmware	Due to the missing permissions on several content providers of the RCS app in its android manifest file will lead to an unprivileged access to phone in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20	2019-05-24	7.2	CVE-2018-13895 CONFIRM
qualcomm -- mdm9150_firmware	Processing messages after error may result in user after free memory fault in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, SM7150	2019-05-24	7.2	CVE-2018-13899 CONFIRM
qualcomm -- mdm9206_firmware	Improper authentication can happen on Remote command handling due to inappropriate handling of events in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SM7150, Snapdragon_High_Med_2016, SXR1130	2019-05-24	7.5	CVE-2018-11271 CONFIRM
qualcomm -- mdm9206_firmware	Index of array is processed in a wrong way inside a while loop and result in invalid index (-1 or something else) leads to out of bound memory access. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA9377, QCA9379, QCA9886, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 820, SD 820A, SD 835, SDX20, SDX24, Snapdragon_High_Med_2016	2019-05-24	10.0	CVE-2018-11936 CONFIRM
qualcomm -- mdm9206_firmware	While updating blacklisting region shared buffered memory region is not validated against newly updated black list, causing boot-up to be compromised in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 615/16/SD 415, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 8CX, SXR1130	2019-05-24	7.2	CVE-2018-12012 CONFIRM
qualcomm -- mdm9206_firmware	Improper authentication in locked memory region can lead to unprivilged access to the memory in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 615/16/SD 415, SD 636, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM630, SDM660, SXR1130	2019-05-24	7.2	CVE-2018-12013 CONFIRM
qualcomm -- mdm9206_firmware	Use-after-free condition due to Improper handling of hrtimers when the PMU driver tries to access its events in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX24	2019-05-24	7.2	CVE-2018-13920 CONFIRM
qualcomm -- mdm9206_firmware	Error in parsing PMT table frees the memory allocated for the map section but does not reset the context map section reference causing heap use after free issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130	2019-05-24	10.0	CVE-2018-13925 CONFIRM

qualcomm -- mdm9206_firmware	Possible integer underflow can happen when calculating length of elementary stream info from invalid section length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearable in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	2019-05-24	10.0	CVE-2019-2244 CONFIRM
qualcomm -- mdm9206_firmware	Possible integer underflow can happen when calculating length of elementary stream map from invalid packet length which is later used to read from input buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, Snapdragon_High_Med_2016	2019-05-24	10.0	CVE-2019-2245 CONFIRM
qualcomm -- qcs605_firmware	Kernel can write to arbitrary memory address passed by user while freeing/stopping a thread in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in QCS605, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SM7150, SXR1130	2019-05-24	7.2	CVE-2019-2250 CONFIRM
s9y -- serendipity	serendipity_moveMediaDirectory in Serendipity 2.0.3 allows remote attackers to upload and execute arbitrary PHP code because it mishandles an extensionless filename during a rename, as demonstrated by “php” as a filename.	2019-05-24	7.5	CVE-2016-10752 MISC MISC
sqlite -- sqlite	SQLite3 from 3.6.0 to and including 3.27.2 is vulnerable to heap out-of-bound read in the rtreenode() function when handling invalid rtree tables.	2019-05-30	7.5	CVE-2019-8457 MISC MISC
synacor -- zimbra_collaboration_suite	ZxChat (aka ZeXtras Chat), as used for zimbra-chat and zimbra-talk in Synacor Zimbra Collaboration Suite 8.7 and 8.8 and in other products, allows XXE attacks, as demonstrated by a crafted XML request to mailboxd.	2019-05-29	7.5	CVE-2018-20160 MISC MISC MISC
synacor -- zimbra_collaboration_suite	Synacor Zimbra Collaboration Suite 8.7.x through 8.8.11 allows insecure object deserialization in the IMAP component.	2019-05-29	7.5	CVE-2019-6980 MISC MISC
synacor -- zimbra_collaboration_suite	mailboxd component in Synacor Zimbra Collaboration Suite 8.7.x before 8.7.11p10 has an XML External Entity injection (XXE) vulnerability.	2019-05-29	7.5	CVE-2019-9670 MISC MISC MISC MISC EXPLOIT-DB
yealink -- ultra-elegant_ip_phone_sip-t41p_firmware	The network diagnostic function (ping) in the Yeahlink Ultra-elegant IP Phone SIP-T41P (firmware 66.83.0.35) allows a remote authenticated attacker to trigger OS commands or open a reverse shell via command injection.	2019-05-29	9.0	CVE-2018-16217 MISC MISC
yealink -- ultra-elegant_ip_phone_sip-t41p_firmware	The diagnostics web interface in the Yeahlink Ultra-elegant IP Phone SIP-T41P (firmware 66.83.0.35) does not validate (escape) the path information (path traversal), which allows an authenticated remote attacker to get access to privileged information (e.g., /etc/passwd) via path traversal (relative path information in the file parameter of the corresponding POST request).	2019-05-29	7.7	CVE-2018-16221 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abantecart -- abantecart	AbanteCart 1.2.8 allows SQL Injection via the source_language parameter to admin/controller/pages/localisation/language.php and core/lib/language_manager.php, or via POST data to admin/controller/pages/tool/backup.php and admin/model/tool/backup.php.	2019-05-24	4.0	CVE-2016-10755 MISC MISC
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7019 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7022 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7023 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7024 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7028 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an integer overflow vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7030 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7032 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7033 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7034 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7035 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7036 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7038 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have a security bypass vulnerability. Successful exploitation could lead to privilege escalation.	2019-05-24	6.8	CVE-2019-7041 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	4.3	CVE-2019-7045 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7047 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	4.3	CVE-2019-7049 CONFIRM

adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7053 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7055 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7056 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7057 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7057 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7058 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7059 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7063 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7064 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7065 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7067 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	4.3	CVE-2019-7071 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	4.3	CVE-2019-7073 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	4.3	CVE-2019-7074 CONFIRM
adobe -- acrobat	Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	5.0	CVE-2019-7081 CONFIRM
adobe -- coldfusion	ColdFusion versions Update 1 and earlier, Update 7 and earlier, and Update 15 and earlier have a cross site scripting vulnerability. Successful exploitation could lead to information disclosure .	2019-05-24	4.3	CVE-2019-7092 CONFIRM
adobe -- creative_cloud	Creative Cloud Desktop Application (installer) versions 4.7.0.400 and earlier have an insecure library loading (dll hijacking) vulnerability. Successful exploitation could lead to privilege escalation.	2019-05-24	6.8	CVE-2019-7093 CONFIRM
adobe -- experience _manager_forms	Adobe Experience Manager Forms versions 6.2, 6.3 and 6.4 have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-05-29	4.3	CVE-2019-7129 CONFIRM
adobe -- flash_player	Flash Player Desktop Runtime versions 32.0.0.114 and earlier, Flash Player for Google Chrome versions 32.0.0.114 and earlier, and Flash Player for Microsoft Edge and Internet Explorer 11 versions 32.0.0.114 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-05-24	4.3	CVE-2019-7090 CONFIRM

afian -- filerun	FileRun 2019.05.21 allows images/extjs Directory Listing	2019-05-30	5.0	CVE-2019-12457 MISC MISC MISC
afian -- filerun	FileRun 2019.05.21 allows css/ext-ux Directory Listing.	2019-05-30	5.0	CVE-2019-12458 MISC MISC MISC
afian -- filerun	FileRun 2019.05.21 allows customizables/plugins/audio_player Directory Listing.	2019-05-30	5.0	CVE-2019-12459 MISC MISC MISC
ampache -- ampache	Ampache 3.8.3 allows PHP Object Instantiation via democratic.ajax.php and democratic.class.php.	2019-05-24	6.5	CVE-2017-18375 MISC
apache -- camel	Apache Camel prior to 2.24.0 contains an XML external entity injection (XXE) vulnerability (CWE-611) due to using an outdated vulnerable JSON-lib library. This affects only the camel-xmljson component, which was removed.	2019-05-28	5.0	CVE-2019-0188 JVN MLIST BID CONFIRM MLIST
apache -- tomcat	The SSI printenv command in Apache Tomcat 9.0.0.M1 to 9.0.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 echoes user provided data without escaping and is, therefore, vulnerable to XSS. SSI is disabled by default. The printenv command is intended for debugging and is unlikely to be present in a production website.	2019-05-28	4.3	CVE-2019-0221 FULLDISC CONFIRM MLIST
bacnet_protocol_stack_project -- bacnet_protocol_stack	BACnet Protocol Stack through 0.8.6 could allow an unauthenticated, remote attacker to cause a denial of service (bacserv daemon crash) because there is an invalid read in bacdcode.c during parsing of alarm tag numbers.	2019-05-30	5.0	CVE-2019-12480 MISC
blueprism -- robotic_process_automation	In AutomateAppCore.dll in Blue Prism Robotic Process Automation 6.4.0.8445, a vulnerability in access control can be exploited to escalate privileges. The vulnerability allows for abusing the application for fraud or unauthorized access to certain information. The attack requires a valid user account to connect to the Blue Prism server, but the roles associated to this account are not required to have any permissions. First of all, the application files are modified to grant full permissions on the client side. In a test environment (or his own instance of the software) an attacker is able to grant himself full privileges also on the server side. He can then, for instance, create a process with malicious behavior and export it to disk. With the modified client, it is possible to import the exported file as a release and overwrite any existing process in the database. Eventually, the bots execute the malicious process. The server does not check the user's permissions for the aforementioned actions, such that a modification of the client software enables this kind of attack. Possible scenarios may involve changing bank accounts or setting passwords.	2019-05-24	6.5	CVE-2019-11875 MISC MISC
bosch -- bosch_video_management_system	A recently discovered security vulnerability affects all Bosch Video Management System (BVMS) versions 9.0 and below, DIVAR IP 2000, 3000, 5000 and 7000, Configuration Manager, Building Integration System (BIS) with Video Engine, Access Professional Edition (APE), Access Easy Controller (AEC), Bosch Video Client (BVC) and Video SDK (VSDK). The RCP+ network port allows access without authentication. Adding authentication feature to the respective library fixes the issue. The issue is classified as "CWE-284: Improper Access Control." This vulnerability, for example, allows a potential attacker to delete video or read video data.	2019-05-29	6.4	CVE-2019-6958 CONFIRM
ca -- risk_authentication	A UI redress vulnerability in the administrative user interface of CA Technologies CA Strong Authentication 9.0.x, 8.2.x, 8.1.x, 8.0.x, 7.1.x and CA Risk Authentication 9.0.x, 8.2.x, 8.1.x, 8.0.x, 3.1.x may allow a remote attacker to gain sensitive information in some cases.	2019-05-28	4.0	CVE-2019-7393 MISC FULLDISC BID BUGTRAQ CONFIRM
ca -- risk_authentication	A privilege escalation vulnerability in the administrative user interface of CA Technologies CA Strong Authentication 9.0.x, 8.2.x, 8.1.x, 8.0.x, 7.1.x and CA Risk Authentication 9.0.x, 8.2.x, 8.1.x, 8.0.x, 3.1.x allows an authenticated attacker to gain additional privileges in some cases where an account has customized and limited privileges.	2019-05-28	6.5	CVE-2019-7394 MISC FULLDISC BID BUGTRAQ CONFIRM
cloudera -- cloudera_manager	An issue was discovered in Cloudera Manager before 5.13.4, 5.14.x before 5.14.4, and 5.15.x before 5.15.1. A read-only user can access sensitive cluster information.T	2019-05-24	4.0	CVE-2018-10815 MISC CONFIRM
computrols -- computrols_building_automation_software	Computrols CBAS 18.0.0 allows Cross-Site Request Forgery.	2019-05-24	6.8	CVE-2018-10847 MISC MISC
computrols -- computrols_building_automation_software	Computrols CBAS 18.0.0 allows Username Enumeration.	2019-05-24	5.0	CVE-2018-10848 MISC MISC
dollarshaveclub -- shave	XSS exists in Shave before 2.5.3 because output encoding is mishandled during the overwrite of an HTML element.	2019-05-24	5.0	CVE-2019-12313 MISC MISC MISC

doxygen -- doxygen	Insufficient sanitization of the query parameter in templates/html/search_opensearch.php could lead to reflected cross-site scripting or iframe injection.	2019-05-24	4.3	CVE-2016-10245 SUSE BID MISC MISC MISC MLIST
drupal -- drupal	In PrestaShop 1.7.5.2, the shop_country parameter in the install/index.php installation script/component is affected by Reflected XSS. Exploitation by a malicious actor requires the user to follow the initial stages of the setup (accepting terms and conditions) before executing the malicious link.	2019-05-24	4.3	CVE-2019-11876 MISC MISC
dynmap_project -- dynmap	In Webbukkit Dynmap 3.0-beta-3, with Spigot 1.13.2, due to a missing login check in servlet/MapStorageHandler.java, an attacker can see a map image without login despite an enabled login-required setting.	2019-05-28	5.0	CVE-2019-12395 MISC MISC MISC
e107 -- e107	e107 2.1.2 allows PHP Object Injection with resultant SQL injection, because usersettings.php uses unserialize without an HMAC.	2019-05-24	6.5	CVE-2016-10753 MISC MISC
eficode -- influxdb	Jenkins InfluxDB Plugin 1.21 and earlier stored credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system.	2019-05-31	4.0	CVE-2019-10329 MLIST MISC
emerson -- ovation_ocr400_firmware	In Emerson Ovation OCR400 Controller 3.3.1 and earlier, a heap-based buffer overflow vulnerability in the embedded third-party FTP server involves improper handling of a long command to the FTP service, which may cause memory corruption that halts the controller or leads to remote code execution and escalation of privileges.	2019-05-28	6.5	CVE-2019-10965 BID MLIST
emerson -- ovation_ocr400_firmware	In Emerson Ovation OCR400 Controller 3.3.1 and earlier, a stack-based buffer overflow vulnerability in the embedded third-party FTP server involves improper handling of a long file name from the LIST command to the FTP service, which may cause the service to overwrite buffers, leading to remote code execution and escalation of privileges.	2019-05-28	6.5	CVE-2019-10967 BID MISC
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/post_note.php has XSS via the garlic_prefix parameter.	2019-05-24	4.3	CVE-2018-12624 MISC CONFIRM
fedoraproject -- fedora	Microarchitectural Store Buffer Data Sampling (MSBDS): Store buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf	2019-05-30	4.7	CVE-2018-12126 FEDORA CONFIRM
fedoraproject -- fedora	Microarchitectural Load Port Data Sampling (MLPDS): Load ports on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf	2019-05-30	4.7	CVE-2018-12127 FEDORA CONFIRM
fedoraproject -- fedora	Microarchitectural Fill Buffer Data Sampling (MFBDS): Fill buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf	2019-05-30	4.7	CVE-2018-12130 FEDORA CONFIRM
fedoraproject -- fedora	Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf	2019-05-30	4.7	CVE-2019-11091 FEDORA CONFIRM
fortinet -- fortianalyzer	An Improper Neutralization of Script-Related HTML Tags in Fortinet FortiAnalyzer 5.6.0 and below and FortiManager 5.6.0 and below allows an attacker to send DHCP request containing malicious scripts in the HOSTNAME parameter. The malicious script code is executed while viewing the logs in FortiAnalyzer and FortiManager (with FortiAnalyzer feature enabled).	2019-05-28	4.3	CVE-2018-13375 CONFIRM
fortinet -- forticlient	A local privilege escalation in Fortinet FortiClient for Windows 6.0.4 and earlier allows attacker to execute unauthorized code or commands via the command injection.	2019-05-30	4.6	CVE-2018-13368 CONFIRM
fortinet -- forticlient	A local privilege escalation in Fortinet FortiClient for Windows 6.0.4 and earlier allows attackers to execute unauthorized code or commands via the named pipe responsible for Forticlient updates.	2019-05-30	4.6	CVE-2018-9191 CONFIRM
fortinet -- forticlient	A local privilege escalation in Fortinet FortiClient for Windows 6.0.4 and earlier allows attacker to execute unauthorized code or commands via the parsing of the file.	2019-05-30	4.6	CVE-2018-9192 CONFIRM
fortinet -- fortios	An Information Exposure vulnerability in Fortinet FortiOS 6.0.1, 5.6.5 and below, allow attackers to learn private IP as well as the hostname of FortiGate via Application Control Block page.	2019-05-29	5.0	CVE-2018-13365 CONFIRM

fortinet -- fortios	A heap buffer overflow in Fortinet FortiOS all versions below 6.0.5 in the SSL VPN web portal may cause the SSL VPN web service termination for logged in users due to a failure to properly handle javascript href data when proxying webpages.	2019-05-29	4.3	CVE-2018-13383 CONFIRM
freeradius -- freeradius	It was discovered freeradius up to and including version 3.0.19 does not correctly configure logrotate, allowing a local attacker who already has control of the radiusd user to escalate his privileges to root, by tricking logrotate into writing a radiusd-writable file to a directory normally inaccessible by the radiusd user.	2019-05-24	6.9	CVE-2019-10143 CONFIRM CONFIRM
gitea -- gitea	Jenkins Gitea Plugin 1.1.1 and earlier did not implement trusted revisions, allowing attackers without commit access to the Git repo to change Jenkinsfiles even if Jenkins is configured to consider them to be untrusted.	2019-05-31	5.0	CVE-2019-10330 MLIST MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition 10.x and 11.x before 11.5.10, 11.6.x before 11.6.8, and 11.7.x before 11.7.3. It has Incorrect Access Control.	2019-05-29	4.0	CVE-2019-7549 MISC MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition 11.x before 11.7.7 and 11.8.x before 11.8.3. It allows Information Disclosure.	2019-05-29	4.0	CVE-2019-9866 MISC
glyphandcog -- xpdfreader	A stack-based buffer over-read exists in FoFiTrueType::dumpString in fofi/FoFiTrueType.cc in Xpdf 4.01.01. It can, for example, be triggered by sending crafted TrueType data in a PDF document to the pdftops tool. It might allow an attacker to cause Denial of Service or leak memory data into dump content.	2019-05-27	5.8	CVE-2019-12360 MISC
glyphandcog -- xpdfreader	A stack-based buffer over-read exists in PostScriptFunction::transform in Function.cc in Xpdf 4.01.01 because GfxSeparationColorSpace and GfxDeviceNColorSpace mishandle tint transform functions. It can, for example, be triggered by sending a crafted PDF document to the pdftops tool. It might allow an attacker to cause Denial of Service or leak memory data.	2019-05-30	5.8	CVE-2019-12493 MISC
gnome -- gvfs	An issue was discovered in GNOME gvfs 1.29.4 through 1.41.2. daemon/gvfsbackendadmin.c has race conditions because the admin backend doesn't implement query_info_on_read/write.	2019-05-29	6.8	CVE-2019-12448 MISC
gpac -- gpac	An issue was discovered in GPAC 0.7.1. There is a NULL pointer dereference in the function GetESD at isomedia/track.c in libgpac.a, as demonstrated by MP4Box.	2019-05-30	4.3	CVE-2019-12481 MISC
gpac -- gpac	An issue was discovered in GPAC 0.7.1. There is a NULL pointer dereference in the function gf_isom_get_original_format_type at isomedia/drm_sample.c in libgpac.a, as demonstrated by MP4Box.	2019-05-30	5.0	CVE-2019-12482 MISC
gpac -- gpac	An issue was discovered in GPAC 0.7.1. There is a heap-based buffer overflow in the function ReadGF_IPMPX_RemoveToolNotificationListener in odf/ipmpx_code.c in libgpac.a, as demonstrated by MP4Box.	2019-05-30	6.8	CVE-2019-12483 MISC
haxx -- curl	An integer overflow in curl's URL API results in a buffer overflow in libcurl 7.62.0 to and including 7.64.1.	2019-05-28	4.3	CVE-2019-5435 CONFIRM
haxx -- libcurl	A heap buffer overflow in the TFTP receiving code allows for DoS or arbitrary code execution in libcurl versions 7.19.4 through 7.64.1.	2019-05-28	4.6	CVE-2019-5436 CONFIRM
heidelberg -- prinect_archiver	A Reflected Cross Site Scripting (XSS) Vulnerability was discovered in Heidelberg Prinect Archiver v2013 release 1.0.	2019-05-24	4.3	CVE-2019-10685 MISC MISC
horde -- groupware	Remote code execution was discovered in Horde Groupware Webmail 5.2.22 and 5.2.17. Horde/Form/Type.php contains a vulnerable class that handles image upload in forms. When the Horde_Form_Type_image method onSubmit() is called on uploads, it invokes the functions getImage() and _getUpload(), which uses unsanitized user input as a path to save the image. The unsanitized POST parameter object[photo][img][file] is saved in the $upload[img][file] PHP variable, allowing an attacker to manipulate the $tmp_file passed to move_uploaded_file() to save the uploaded file. By setting the parameter to (for example) ../usr/share/horde/static/bd.php, one can write a PHP backdoor inside the web root. The static/ destination folder is a good candidate to drop the backdoor because it is always writable in Horde installations. (The unsanitized POST parameter went probably unnoticed because it's never submitted by the forms, which default to securely using a random path.)	2019-05-29	6.5	CVE-2019-9858 MISC MISC
hybridgroup -- gobot	An issue was discovered in Hybrid Group Gobot before 1.13.0. The mqtt subsystem skips verification of root CA certificates by default.	2019-05-31	5.0	CVE-2019-12496 MISC MISC
ibm -- api_connect	IBM API Connect 5.0.0.0 through 5.0.8.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 159944.	2019-05-29	5.0	CVE-2019-4256 BID XF CONFIRM
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.2.8 WinCollect could allow an attacker to obtain sensitive information by spoofing a trusted entity using man in the middle techniques due to not validating or incorrectly validating a certificate. IBM X-Force ID: 160072.	2019-05-29	4.3	CVE-2019-4264 BID XF CONFIRM

incsub -- hustle	The Hustle (aka wordpress-popup) plugin 6.0.7 for WordPress is vulnerable to CSV Injection as it allows for injecting malicious code into a pop-up window. Successful exploitation grants an attacker with a right to execute malicious code on the administrator's computer through Excel functions as the plugin does not sanitize the user's input and allows insertion of any text.	2019-05-29	6.8	CVE-2019-11872 MISC MISC MISC
jenkins -- pipeline_maven_integration	An XML external entities (XXE) vulnerability in Jenkins Pipeline Maven Integration Plugin 1.7.0 and earlier allowed attackers able to control a temporary directory's content on the agent running the Maven build to have Jenkins parse a maliciously crafted XML file that uses external entities for extraction of secrets from the Jenkins master, server-side request forgery, or denial-of-service attacks.	2019-05-31	5.5	CVE-2019-10327 MLIST MISC
jenkins -- pipeline_maven_integration	Jenkins Pipeline Remote Loader Plugin 1.4 and earlier provided a custom whitelist for script security that allowed attackers to invoke arbitrary methods, bypassing typical sandbox protection.	2019-05-31	6.5	CVE-2019-10328 MLIST MISC
jenkins -- pipeline_maven_integration	Jenkins Pipeline Remote Loader Plugin 1.4 and earlier provided a custom whitelist for script security that allowed attackers to invoke arbitrary methods, bypassing typical sandbox protection.	2019-05-31	6.5	CVE-2019-10328 MLIST MISC
jenkins -- warnings_next_generation	A cross-site request forgery vulnerability in Jenkins Warnings NG Plugin 5.0.0 and earlier allowed attackers to reset warning counts for future builds.	2019-05-31	4.3	CVE-2019-10326 MLIST MISC
jfrog -- artifactory	A cross-site request forgery vulnerability in Jenkins Artifactory Plugin 3.2.2 and earlier in ArtifactoryBuilder.DescriptorImpl#doTestConnection allowed users with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-05-31	4.3	CVE-2019-10321 MLIST MISC
jfrog -- artifactory	A missing permission check in Jenkins Artifactory Plugin 3.2.2 and earlier in ArtifactoryBuilder.DescriptorImpl#doTestConnection allowed users with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-05-31	4.0	CVE-2019-10322 MLIST MISC
jfrog -- artifactory	A cross-site request forgery vulnerability in Jenkins Artifactory Plugin 3.2.2 and earlier in ReleaseAction#doSubmit, GradleReleaseApiAction#doStaging, MavenReleaseApiAction#doStaging, and UnifiedPromoteBuildAction#doSubmit allowed attackers to schedule a release build, perform release staging for Gradle and Maven projects, and promote previously staged builds, respectively.	2019-05-31	4.3	CVE-2019-10324 MLIST MISC
kibokolabs -- hostel	XSS exists in the Kiboko Hostel plugin before 1.1.4 for WordPress.	2019-05-27	4.3	CVE-2019-12345 MISC
kliqqi -- kliqqi_cms	Kliqqi 3.0.0.5 allows CSRF with resultant Arbitrary File Upload because module.php?module=upload can be used to configure the uploading of .php files, and then modules/upload/upload_main.php can be used for the upload itself.	2019-05-24	6.8	CVE-2016-10756 MISC MISC
linux -- linux_kernel	An issue was discovered in ip6_ra_control in net/ipv6/ipv6_sockglue.c in the Linux kernel through 5.1.5. There is an unchecked kmalloc of new_ra, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash).	2019-05-27	4.9	CVE-2019-12378 BID MISC MISC
linux -- linux_kernel	An issue was discovered in con_insert_unipair in drivers/tty/vt/consolemap.c in the Linux kernel through 5.1.5. There is a memory leak in a certain case of an ENOMEM outcome of kmalloc.	2019-05-27	4.9	CVE-2019-12379 BID MISC
linux -- linux_kernel	An issue was discovered in ip_ra_control in net/ipv4/ip_sockglue.c in the Linux kernel through 5.1.5. There is an unchecked kmalloc of new_ra, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash).	2019-05-27	4.9	CVE-2019-12381 BID MISC MISC
linux -- linux_kernel	An issue was discovered in drm_load_edid_firmware in drivers/gpu/drm/drm_edid_load.c in the Linux kernel through 5.1.5. There is an unchecked kstrdup of fwstr, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash).	2019-05-27	4.9	CVE-2019-12382 BID MISC MISC
linux -- linux_kernel	An issue was discovered in sunxi_divs_clk_setup in drivers/clk/sunxi/clk-sunxi.c in the Linux kernel through 5.1.5. There is an unchecked kstrndup of derived_name, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash).	2019-05-30	4.9	CVE-2019-12455 MISC MISC
netgate -- pfsense	In pfSense 2.4.4-p3, a stored XSS vulnerability occurs when attackers inject a payload into the Name or Description field via an acme_accountkeys_edit.php action. The vulnerability occurs due to input validation errors.	2019-05-29	4.3	CVE-2019-12347 MISC MISC CONFIRM MISC MISC
oracle -- enterprise_manager_ops_center	Vulnerability in the Enterprise Manager Ops Center component of Oracle Enterprise Manager Products Suite (subcomponent: Services Integration). The supported version that is affected is 12.3.3. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager Ops Center. While the vulnerability is in Enterprise Manager Ops Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Enterprise Manager Ops Center. CVSS 3.0 Base Score 6.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:N/A:H).	2019-05-24	6.3	CVE-2019-2726 MISC

osclass -- osclass	osClass 3.6.1 allows oc-admin/plugins.php Directory Traversal via the plugin parameter. This is exploitable for remote PHP code execution because an administrator can upload an image that contains PHP code in the EXIF data via index.php?page=ajax&action=ajax_upload.	2019-05-24	6.5	CVE-2016-10751 MISC MISC
phome -- empirecms	EmpireCMS 7.5.0 has XSS via the from parameter to e/member/doaction.php, as demonstrated by a CSRF payload that changes the dynamic page template. The attacker can choose to resend the e/template/member/regsend.php registered activation mail page.	2019-05-27	4.3	CVE-2019-12361 MISC
phome -- empirecms	EmpireCMS 7.5.0 has XSS via the HTTP Referer header to e/member/doaction.php.	2019-05-27	4.3	CVE-2019-12362 MISC
phpkit -- phpkit	PHPKIT 1.6.6 allows arbitrary File Upload, as demonstrated by a .php file to pkinc/admin/mediaarchive.php and pkinc/func/default.php via the image_name parameter.	2019-05-24	6.5	CVE-2016-10758 MISC MISC
phprelativepath_project -- phprelativepath	An XSS vulnerability exists in PHPRelativePath (aka Relative Path) through 1.0.2 via the RelativePath.Example1.php path parameter.	2019-05-31	4.3	CVE-2019-12507 MISC MISC
qemu -- qemu	interface_release_resource in hw/display/qxl.c in QEMU 4.0.0 has a NULL pointer dereference.	2019-05-24	5.0	CVE-2019-12155 CONFIRM MISC BUGTRAQ DEBIAN
qualcomm -- 215_firmware	Buffer overflow can occur if invalid header tries to overwrite the existing buffer which fix size allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 820, SD 820A, SD 845 / SD 850, SDM439, SDM660, SDX20	2019-05-24	4.6	CVE-2019-2248 CONFIRM
qualcomm -- ipq8074_firmware	ECDSA signature code leaks private keys from secure world to non-secure world in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130	2019-05-24	4.9	CVE-2018-11976 CONFIRM
qualcomm -- mdm9150_firmware	Improper buffer length check before copying can lead to integer overflow and then a buffer overflow in WMA event handler in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6574AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24	2019-05-24	4.6	CVE-2018-11923 CONFIRM
qualcomm -- mdm9150_firmware	Improper buffer length validation in WLAN function can lead to a potential integer oveflow issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SM7150	2019-05-24	4.6	CVE-2018-11924 CONFIRM
qualcomm -- mdm9150_firmware	An unprivileged user can issue a binder call and cause a system halt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, SM7150	2019-05-24	4.9	CVE-2018-12005 CONFIRM
qualcomm -- mdm9150_firmware	Possible memory overread may be lead to access of sensitive data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9650, MDM9655, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, SDX20, SM7150, SXR1130	2019-05-24	4.9	CVE-2018-13885 CONFIRM
qualcomm -- mdm9150_firmware	Possibility of double free issue while running multiple instances of smp2p test because of proper protection is missing while using global variable in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	2019-05-24	4.6	CVE-2019-2247 CONFIRM

qualcomm -- mdm9206_firmware	Secure keypad is unlocked with secure display still intact in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 615/16/SD 415, SD 636, SD 712 / SD 710 / SD 670, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM630, SDM660, SXR1130	2019-05-24	4.9	CVE-2018-12004 CONFIRM
readaxo -- readaxo	In Redaxo 5.2.0, the cron management of the admin panel suffers from CSRF that leads to arbitrary Remote Code Execution via addons/cronjob/lib/types/phpcode.php.	2019-05-24	6.8	CVE-2016-10757 MISC MISC
revive-adserver -- revive_adserver	Use of cryptographically weak PRNG in the password recovery token generation of Revive Adserver < v4.2.1 causes a potential authentication bypass attack if an attacker exploits the password recovery functionality. In lib/OA/Dal/PasswordRecovery.php, the function generateRecoveryId() generates a password reset token that relies on the PHP uniqid function and consequently depends only on the current server time, which is often visible in an HTTP Date header.	2019-05-28	6.8	CVE-2019-5440 MISC
samsung -- scx-824_firmware	Samsung SCX-824 printers allow a reflected Cross-Site-Scripting (XSS) vulnerability that can be triggered by using the “print from file” feature, as demonstrated by the sws/swsAlert.sws?popupid=successMsg msg parameter.	2019-05-24	4.3	CVE-2019-12315 MISC
synacor -- zimbra_collaboration_suite	Synacor Zimbra Mail Client 8.6 before 8.6.0 Patch 5 has XSS via the error/warning dialog and email body content in Zimbra.	2019-05-30	4.3	CVE-2015-7609 MISC MISC MISC MISC MISC
synacor -- zimbra_collaboration_suite	Synacor Zimbra Collaboration Suite Collaboration before 8.8.11 has XSS in the AJAX and html web clients.	2019-05-29	4.3	CVE-2018-14013 MISC MISC MISC MISC MISC MISC MISC
synacor -- zimbra_collaboration_suite	There is a Persistent XSS vulnerability in the briefcase component of Synacor Zimbra Collaboration Suite (ZCS) Zimbra Web Client (ZWC) 8.8.8 before 8.8.8 Patch 7 and 8.8.9 before 8.8.9 Patch 1.	2019-05-30	4.3	CVE-2018-14425 MISC MISC
synacor -- zimbra_collaboration_suite	An issue was discovered in Synacor Zimbra Collaboration Suite 8.6.x before 8.6.0 Patch 11, 8.7.x before 8.7.11 Patch 6, 8.8.x before 8.8.8 Patch 9, and 8.8.9 before 8.8.9 Patch 3. Account number enumeration is possible via inconsistent responses for specific types of authentication requests.	2019-05-30	5.0	CVE-2018-15131 MISC MISC
synacor -- zimbra_collaboration_suite	mailboxd component in Synacor Zimbra Collaboration Suite 8.6, 8.7 before 8.7.11 Patch 7, and 8.8 before 8.8.10 Patch 2 has Persistent XSS.	2019-05-29	4.3	CVE-2018-18631 MISC MISC
synacor -- zimbra_collaboration_suite	Zimbra Collaboration Suite 8.7.x through 8.8.11 allows Blind SSRF in the Feed component.	2019-05-29	4.0	CVE-2019-6981 MISC MISC
tinycc -- tinycc	An issue was discovered in Tiny C Compiler (aka TinyCC or TCC) 0.9.27. Compiling a crafted source file leads to a one-byte out-of-bounds write in the gsym_addr function in x86_64-gen.c. This occurs because tccasm.c mishandles section switches.	2019-05-31	4.3	CVE-2019-12495 MISC MISC
torproject -- tor_browser	Tor Browser before 8.0.1 has an information exposure vulnerability. It allows remote attackers to detect the browser’s UI locale by measuring a button width, even if the user has a “Don’t send my language” setting.	2019-05-27	4.3	CVE-2019-12383 BID MISC MISC MISC
vtiger -- vtiger_crm	modules/Calendar/Activity.php in Vtiger CRM 6.5.0 allows SQL injection via the contactidlist parameter.	2019-05-24	6.5	CVE-2016-10754 MISC MISC
webport -- web_port	Web Port 1.19.1 allows XSS via the /access/setup type parameter.	2019-05-30	4.3	CVE-2019-12460 MISC MISC
webport -- web_port	Web Port 1.19.1 allows XSS via the /log type parameter.	2019-05-30	4.3	CVE-2019-12461 MISC MISC
westermo -- dr-250_firmware	The /uploadfile? functionality in Westermo DR-250 Pre-5162 and DR-260 Pre-5162 routers allows remote users to upload malicious file types and execute ASP code.	2019-05-24	6.5	CVE-2018-19612 MISC MISC
westermo -- dr-250_firmware	Westermo DR-250 Pre-5162 and DR-260 Pre-5162 routers allow CSRF.	2019-05-24	4.3	CVE-2018-19613 MISC MISC
windriver -- vxworks	When RPC is enabled in Wind River VxWorks 6.9 prior to 6.9.1, a specially crafted RPC request can trigger an integer overflow leading to an out-of-bounds memory copy. It may allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code.	2019-05-29	6.8	CVE-2019-9865 MISC CONFIRM

yealink -- ultra-elegant_ip_phone_sip-t41p_firmware	A CSRF (Cross Site Request Forgery) in the web interface of the Yealink Ultra-elegant IP Phone SIP-T41P firmware version 66.83.0.35 allows a remote attacker to trigger code execution or settings modification on the device by providing a crafted link to the victim.	2019-05-29	6.8	CVE-2018-16218 MISC MISC
zohocorp -- manageengine_adself-service_plus	In Zoho ManageEngine ADSelfService Plus 5.x through 5704, an authorization.do cross-site Scripting (XSS) vulnerability allows for an unauthenticated manipulation of the JavaScript code by injecting the HTTP form parameter adscsrf. An attacker can use this to capture a user's AD self-service password reset and MFA token.	2019-05-24	4.3	CVE-2019-8346 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 3 of 5).	2019-05-29	2.1	CVE-2019-9221 MISC MISC
iball -- 300m_2-port_wireless-n_broadband_router_firmware	iBall Baton iB-WRB302N20122017 devices have improper access control over the UART interface, allowing physical attackers to discover Wi-Fi credentials (plain text) and the web-console password (base64) via the debugging console.	2019-05-28	2.1	CVE-2018-20008 MISC MISC
ibm -- cognos_analytics	IBM Cognos Analytics 11.0, 11.1.0, and 11.1.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158335.	2019-05-29	3.5	CVE-2019-4139 CONFIRM BID XF
ibm -- jazz_reporting_service	IBM Jazz Reporting Service 6.0 through 6.0.6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158974.	2019-05-29	3.5	CVE-2019-4184 BID XF CONFIRM
jenkins -- warnings_next_generation	A cross-site scripting vulnerability in Jenkins Warnings NG Plugin 5.0.0 and earlier allowed attacker with Job/Configure permission to inject arbitrary JavaScript in build overview pages.	2019-05-31	3.5	CVE-2019-10325 MLIST MISC
linux -- linux_kernel	An issue was discovered in the efi subsystem in the Linux kernel through 5.1.5. phys_efi_set_virtual_address_map in arch/x86/platform/efi/efi.c and efi_call_phys_prolog in arch/x86/platform/efi/efi_64.c mishandle memory allocation failures.	2019-05-27	2.1	CVE-2019-12380 BID MISC
synacor -- zimbra_collaboration_suite	Synacor Zimbra Admin UI in Zimbra Collaboration Suite before 8.8.0 beta 2 has Persistent XSS via mail addrs.	2019-05-30	3.5	CVE-2018-10948 MISC
tp-link -- tl-wr840n_firmware	TP-Link TL-WR840N v5 00000005 devices allow XSS via the network name. The attacker must log into the router by breaking the password and going to the admin login page by THC-HYDRA to get the network name. With an XSS payload, the network name changed automatically and the internet connection was disconnected. All the users become disconnected from the internet.	2019-05-24	3.5	CVE-2019-12195 MISC MISC

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
advanced_infodata_systems -- esel-server	SQL Injection in Advanced InfoData Systems (AIS) ESEL-Server 67 (which is the backend for the AIS logistics mobile app) allows an anonymous attacker to execute arbitrary code in the context of the user of the MSSQL database. The default user for the database is the 'sa' user.	2019-05-31	not yet calculated	CVE-2019-10123 MISC MISC
apache -- roller	Server-side Request Forgery (SSRF) and File Enumeration vulnerability in Apache Roller 5.2.1, 5.2.0 and earlier unsupported versions relies on Java SAX Parser to implement its XML-RPC interface and by default that parser supports external entities in XML DOCTYPE, which opens Roller up to SSRF / File Enumeration vulnerability. Note that this vulnerability exists even if Roller XML-RPC interface is disable via the Roller web admin UI. Mitigation: There are a couple of ways you can fix this vulnerability: 1) Upgrade to the latest version of Roller, which is now 5.2.2 2) Or, edit the Roller web.xml file and comment out the XML-RPC Servlet mapping as shown below: <!-- <servlet-mapping> <servlet-name>XmlRpcServlet</servlet-name> <url-pattern>/roller-services/xmlrpc</url-pattern> </servlet-mapping> -->	2019-05-28	not yet calculated	CVE-2018-17198 BID MISC
aveva -- vijeo_citect_and_citectscada	In Vijeo Citect 7.30 and 7.40, and CitectSCADA 7.30 and 7.40, a vulnerability has been identified that may allow an authenticated local user access to Citect user credentials.	2019-05-31	not yet calculated	CVE-2019-10981 MISC CONFIRM
bitdefender -- bitdefender_engines	An issue was discovered in Bitdefender Engines before 7.76675. A vulnerability has been discovered in the rar.xmd parser that results from a lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. Paired with other vulnerabilities, this can result in denial-of-service. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	2019-05-24	not yet calculated	CVE-2018-18059 MISC MISC

bitdefender -- bitdefender_engines	An issue was discovered in Bitdefender Engines before 7.76808. A vulnerability has been discovered in the dalvik.xmd parser that results from a lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. Paired with other vulnerabilities, this can result in denial-of-service. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	2019-05-24	not yet calculated	CVE-2018-18060 MISC MISC
bitdefender -- bitdefender_engines	An issue was discovered in Bitdefender Engines before 7.76662. A vulnerability has been discovered in the iso.xmd parser that results from a lack of proper validation of user-supplied data, which can result in a division-by-zero circumstance. Paired with other vulnerabilities, this can result in denial-of-service. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	2019-05-24	not yet calculated	CVE-2018-18058 MISC MISC
bosch -- smart_home_controller	A potential improper access control vulnerability exists in the JSON-RPC interface of the Bosch Smart Home Controller (SHC) before 9.8.905 that may result in reading or modification of the SHC's configuration or triggering and restoring backups. In order to exploit the vulnerability, the adversary needs to have successfully paired an app or service, which requires user interaction.	2019-05-29	not yet calculated	CVE-2019-11892 CONFIRM
bosch -- smart_home_controller	A potential incorrect privilege assignment vulnerability exists in the app pairing mechanism of the Bosch Smart Home Controller (SHC) before 9.8.905 that may result in elevated privileges of the adversary's choosing. In order to exploit the vulnerability, the adversary needs physical access to the SHC during the attack.	2019-05-29	not yet calculated	CVE-2019-11891 CONFIRM
bosch -- smart_home_controller	A potential incorrect privilege assignment vulnerability exists in the app permission update API of the Bosch Smart Home Controller (SHC) before 9.8.905 that may result in a restricted app obtaining default app permissions. In order to exploit the vulnerability, the adversary needs to have successfully paired an app with restricted permissions, which required user interaction.	2019-05-29	not yet calculated	CVE-2019-11893 CONFIRM
bosch -- smart_home_controller	A potential improper access control vulnerability exists in the backup mechanism of the Bosch Smart Home Controller (SHC) before 9.8.905 that may result in unauthorized download of a backup. In order to exploit the vulnerability, the adversary needs to download the backup directly after a backup triggered by a legitimate user has been completed.	2019-05-29	not yet calculated	CVE-2019-11894 CONFIRM
bosch -- smart_home_controller	A potential improper access control vulnerability exists in the JSON-RPC interface of the Bosch Smart Home Controller (SHC) before 9.8.905 that may result in a successful denial of service of the SHC and connected sensors and actuators. In order to exploit the vulnerability, the adversary needs to have successfully paired an app or service, which requires user interaction.	2019-05-29	not yet calculated	CVE-2019-11895 CONFIRM
bosch -- smart_home_controller	A potential incorrect privilege assignment vulnerability exists in the 3rd party pairing mechanism of the Bosch Smart Home Controller (SHC) before 9.8.907 that may result in a restricted app obtaining default app permissions. In order to exploit the vulnerability, the adversary needs to have successfully paired an app, which requires user interaction.	2019-05-29	not yet calculated	CVE-2019-11896 CONFIRM
containous -- traefik	types/types.go in Containous Traefik 1.7.x through 1.7.11, when the --api flag is used and the API is publicly reachable and exposed without sufficient access control (which is contrary to the API documentation), allows remote authenticated users to discover password hashes by reading the Basic HTTP Authentication or Digest HTTP Authentication section, or discover a key by reading the ClientTLS section. These can be found in the JSON response to a /api request.	2019-05-29	not yet calculated	CVE-2019-12452 MISC MISC MISC
evernote -- evernote	Evernote 7.9 on macOS allows attackers to execute arbitrary programs by embedding a reference to a local executable file such as the /Applications/Calculator.app/Contents/MacOS/Calculator file.	2019-05-31	not yet calculated	CVE-2019-10038 MISC MISC MISC
godot_engine -- godot	In Godot through 3.1, remote code execution is possible due to the deserialization policy not being applied correctly.	2019-05-31	not yet calculated	CVE-2019-10069 MISC MISC
google -- sign-in	An unhandled exception vulnerability exists during Google Sign-In with Google API C++ Client before 2019-04-10. It potentially causes an outage of third-party services that were not designed to recover from exceptions. On the client, ID token handling can cause an unhandled exception because of misinterpretation of an integer as a string, resulting in denial-of-service and then other users can no longer login/sign-in to the affected third-party service. Once this third-party service uses Google Sign-In with google-api-cpp-client, a malicious user can trigger this client/auth/oauth2_authorization.cc vulnerability by requesting the client to receive the ID token from a Google authentication server.	2019-05-30	not yet calculated	CVE-2018-20840 MISC MISC
hp -- workstation_bios	HP has identified a security vulnerability with some versions of Workstation BIOS (UEFI Firmware) where the runtime BIOS code could be tampered with if the TPM is disabled. This vulnerability relates to Workstations whose TPM is enabled by default.	2019-05-29	not yet calculated	CVE-2019-6322 HP
hp -- workstation_bios	HP has identified a security vulnerability with some versions of Workstation BIOS (UEFI Firmware) where the runtime BIOS code could be tampered with if the TPM is disabled. This vulnerability relates to Workstations whose TPM is disabled by default.	2019-05-29	not yet calculated	CVE-2019-6321 HP
ibm -- spectrum_control	IBM Tivoli Storage Productivity Center 5.2.13 through 5.3.0.1 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. X-Force ID: 158334.	2019-05-29	not yet calculated	CVE-2019-4138 CONFIRM BID XF

ibm -- spectrum_control	IBM Tivoli Storage Productivity Center 5.2.13 through 5.3.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158333.	2019-05-29	not yet calculated	CVE-2019-4137 CONFIRM BID XF
jector -- smart_tv_fm-k75_devices	Jector Smart TV FM-K75 devices allow remote code execution because there is an adb open port with root permission.	2019-05-31	not yet calculated	CVE-2019-9871 MISC MISC
logicaldoc -- logicaldoc_community_edition	LogicalDOC Community Edition 8.x before 8.2.1 has a path traversal vulnerability that allows reading arbitrary files and the creation of directories, in the class PluginRegistry.	2019-05-30	not yet calculated	CVE-2019-9723 MISC
mitel -- micollab_and_micollab_awv	MiCollab 7.3 PR2 (7.3.0.204) and earlier, 7.2 (7.2.2.13) and earlier, and 7.1 (7.1.0.57) and earlier and MiCollab AWV 6.3 (6.3.0.103), 6.2 (6.2.2.8), 6.1 (6.1.0.28), 6.0 (6.0.0.61), and 5.0 (5.0.5.7) have a Command Execution Vulnerability. Successful exploit of this vulnerability could allow an attacker to execute arbitrary system commands.	2019-05-29	not yet calculated	CVE-2019-12165 MISC
nuuo -- network_video_recorder_firmware	NUUO Network Video Recorder Firmware 1.7.x through 3.3.x allows unauthenticated attackers to execute arbitrary commands via shell metacharacters to handle_load_config.php.	2019-05-31	not yet calculated	CVE-2019-9653 MISC MISC MISC
nvidia -- geforce_experience	NVIDIA GeForce Experience versions prior to 3.19 contains a vulnerability in the Web Helper component, in which an attacker with local system access can craft input that may not be properly validated. Such an attack may lead to code execution, denial of service or information disclosure.	2019-05-31	not yet calculated	CVE-2019-5678 CONFIRM
petraware -- ptransformer_adc	Petraware pTransformer ADC before 2.1.7.22827 allows SQL Injection via the User ID parameter to the login form.	2019-05-27	not yet calculated	CVE-2019-12372 MISC MISC
project_atomic -- bubblewrap	bubblewrap.c in Bubblewrap before 0.3.3 misuses temporary directories in /tmp as a mount point. In some particular configurations (related to XDG_RUNTIME_DIR), a local attacker may abuse this flaw to prevent other users from executing bubblewrap or potentially execute code.	2019-05-29	not yet calculated	CVE-2019-12439 MISC MISC MISC MISC
pydio -- pydio	An unauthenticated attacker can obtain information about the Pydio 8.2.2 configuration including session timeout, libraries, and license information.	2019-05-31	not yet calculated	CVE-2019-10046 MISC
pydio -- pydio	The “action” get_sess_id in the web application of Pydio through 8.2.2 discloses the session cookie value in the response body, enabling scripts to get access to its value. This identifier can be reused by an attacker to impersonate a user and perform actions on behalf of him/her (if the session is still active).	2019-05-31	not yet calculated	CVE-2019-10045 MISC
pydio -- pydio	It is possible for an attacker with regular user access to the web application of Pydio through 8.2.2 to trick an administrator user into opening a link shared through the application, that in turn opens a shared file that contains JavaScript code (that is executed in the context of the victim user to obtain sensitive information such as session identifiers and perform actions on behalf of him/her).	2019-05-31	not yet calculated	CVE-2019-10049 MISC
pydio -- pydio	A stored XSS vulnerability exists in the web application of Pydio through 8.2.2 that can be exploited by levering the file upload and file preview features of the application. An authenticated attacker can upload an HTML file containing JavaScript code and afterwards a file preview URL can be used to access the uploaded file. If a malicious user shares an uploaded HTML file containing JavaScript code with another user of the application, and tricks an authenticated victim into accessing a URL that results in the HTML code being interpreted by the web browser, then the included JavaScript code is executed under the context of the victim user session.	2019-05-31	not yet calculated	CVE-2019-10047 MISC
pydio -- pydio	The ImageMagick plugin that is installed by default in Pydio through 8.2.2 does not perform the appropriate validation and sanitization of user supplied input in the plugin’s configuration options, allowing arbitrary shell commands to be entered that result in command execution on the underlying operating system, with the privileges of the local user running the web server. The attacker must be authenticated into the application with an administrator user account in order to be able to edit the affected plugin configuration.	2019-05-31	not yet calculated	CVE-2019-10048 MISC
qemu -- qemu	In QEMU 3.1.0, load_device_tree in device_tree.c calls the deprecated load_image function, which has a buffer overflow risk.	2019-05-31	not yet calculated	CVE-2018-20815 MISC
quest -- kace_systems_management_appliance	An issue was discovered in Quest KACE Systems Management Appliance before 9.1. The script at /service/kbot_service_notsoap.php is vulnerable to unauthenticated reflected XSS when user-supplied input to the METHOD GET parameter is processed by the web application. Since the application does not properly validate and sanitize this parameter, it is possible to place arbitrary script code into the context of the same page.	2019-05-24	not yet calculated	CVE-2019-11604 MISC FULLDISC MISC

saet -- impianti_speciali_tebe_small_devices	The WebApp v04.68 in the supervisor on SAET Impianti Speciali TEBE Small 05.01 build 1137 devices allows remote attackers to execute or include local .php files, as demonstrated by menu=php://filter/convert.base64-encode/resource=index.php to read index.php.	2019-05-31	not yet calculated	CVE-2019-9106 MISC MISC
saet -- impianti_speciali_tebe_small_devices	The WebApp v04.68 in the supervisor on SAET Impianti Speciali TEBE Small 05.01 build 1137 devices allows remote attackers to make several types of API calls without authentication, as demonstrated by retrieving password hashes via an inc/utils/REST_API.php?command=-CallAPI&customurl=alladminusers call.	2019-05-31	not yet calculated	CVE-2019-9105 MISC MISC
sitecore -- sitecore	Deserialization of Untrusted Data in the anti CSRF module in Sitecore through 9.1 allows an authenticated attacker to execute arbitrary code by sending a serialized .NET object in an HTTP POST parameter.	2019-05-31	not yet calculated	CVE-2019-9875 MISC MISC MISC
sitecore -- sitecore_cms_and_sitecore_xp	Deserialization of Untrusted Data in the Sitecore.Security.AntiCSRF (aka anti CSRF) module in Sitecore CMS 7.0 to 7.2 and Sitecore XP 7.5 to 8.2 allows an unauthenticated attacker to execute arbitrary code by sending a serialized .NET object in the HTTP POST parameter __CSRFTOKEN.	2019-05-31	not yet calculated	CVE-2019-9874 MISC MISC MISC
sitecore -- sitecore_rocks	The Sitecore Rocks plugin before 2.1.149 for Sitecore allows an unauthenticated threat actor to inject malicious commands and code via the Sitecore Rocks Hard Rocks Service.	2019-05-29	not yet calculated	CVE-2019-12440 MISC MISC MISC
synacor -- zimbra_collaboration_server	Synacor Zimbra Collaboration Server 8.x before 8.7.0 has Reflected XSS in admin console.	2019-05-30	not yet calculated	CVE-2015-2230 MISC MISC
the_linux_documentation_project -- advanced_bash_scripting_guide	The function getopt_simple as described in Advanced Bash Scripting Guide (ISBN 978-1435752184) allows privilege escalation and execution of commands when used in a shell script called, for example, via sudo.	2019-05-31	not yet calculated	CVE-2019-9891 MISC
xiaomi -- m365_scooter	The Xiaomi M365 scooter 2019-02-12 before 1.5.1 allows spoofing of “suddenly accelerate” commands. This occurs because Bluetooth Low Energy commands have no server-side authentication check. Other affected commands include suddenly braking, locking, and unlocking.	2019-05-31	not yet calculated	CVE-2019-12500 MISC
xpdf -- xpdf	There is an out-of-bounds read vulnerability in the function FlateStream::getChar() located at Stream.cc in Xpdf 4.01.01. It can, for example, be triggered by sending a crafted PDF document to the pdftoppm tool. It might allow an attacker to cause Information Disclosure or a denial of service.	2019-06-01	not yet calculated	CVE-2019-12515 MISC
zyxel -- p-660hn_t1_devices	The rpWLANRedirect.asp ASP page is accessible without authentication on ZyXEL P-660HN-T1 V2 (2.00(AAKK.3)) devices. After accessing the page, the admin user’s password can be obtained by viewing the HTML source code, and the interface of the modem can be accessed as admin.	2019-06-01	not yet calculated	CVE-2019-6725 BUGTRAQ