Vulnerability Summary for the Week of July 15, 2019

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

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

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

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
contao -- contao	Contao 4.x allows SQL Injection. Fixed in Contao 4.4.39 and Contao 4.7.5.	2019-07-09	7.5	CVE-2019-11512 MISC
dlink -- central_wifimanager	/web/Lib/Action/IndexAction.class.php in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 allows remote attackers to execute arbitrary PHP code via a cookie because a cookie's username field allows eval injection, and an empty password bypasses authentication.	2019-07-06	7.5	CVE-2019-13372 MISC CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dlink -- central_wifimanager	An issue was discovered in the D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6. Input does not get validated and arbitrary SQL statements can be executed in the database via the /web/Public/Conn.php parameter dbSQL.	2019-07-06	7.5	CVE-2019-13373 MISC CONFIRM MISC
dlink -- central_wifimanager	A SQL Injection was discovered in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 in PayAction.class.php with the index.php/Pay/passcodeAuth parameter passcode. The vulnerability does not need any authentication.	2019-07-06	7.5	CVE-2019-13375 MISC CONFIRM MISC
dlink -- dir-655_firmware	D-Link DIR-655 C devices before 3.02B05 BETA03 allow remote attackers to execute arbitrary commands via shell metacharacters in the online_firmware_check.cgi check_fw_url parameter.	2019-07-11	10.0	CVE-2019-13561 MISC MISC MISC
dlink -- dir-818lw_firmware	An issue was discovered on D-Link DIR-818LW devices with firmware 2.06betab01. There is a command injection in HNAP1 (exploitable with Authentication) via shell metacharacters in the MTU field to SetWanSettings.	2019-07-10	9.0	CVE-2019-13481 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dlink -- dir-818lw_firmware	An issue was discovered on D-Link DIR-818LW devices with firmware 2.06betab01. There is a command injection in HNAP1 (exploitable with Authentication) via shell metacharacters in the Type field to SetWanSettings.	2019-07-10	10.0	CVE-2019-13482 BID MISC
fortinet -- fcm-mb40_firmware	Dynacolor FCM-MB40 v1.2.0.0 devices allow remote attackers to execute arbitrary commands via a crafted parameter to a CGI script, as demonstrated by sed injection in cgi-bin/camctrl_save_profile.cgi (save parameter) and cgi-bin/ddns.cgi.	2019-07-07	9.0	CVE-2019-13398 MISC
google -- android	In ihevcd_sao_shift_ctb of ihevcd_sao.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-130023983.	2019-07-08	9.3	CVE-2019-2106 CONFIRM
google -- android	In ihevcd_parse_pps of ihevcd_parse_headers.c, there	2019-07-08	9.3	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-130024844.			2107 CONFIRM
google -- android	In MakeMPEG4VideoCodecSpecificData of AVIExtractor.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1. Android ID: A-130651570.	2019-07-08	9.3	CVE-2019-2109 CONFIRM
google -- android	In loop of DnsTlsSocket.cpp, there is a possible heap memory corruption due to a use after free. This could lead to remote code execution in the netd server with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-07-08	7.5	CVE-2019-2111 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Product: Android. Versions: Android-9. Android ID: A-122856181.			
google -- android	In several functions of alarm.cc, there is possible memory corruption due to a use after free. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-117997080.	2019-07-08	7.2	CVE-2019-2112 CONFIRM
hidea -- az_admin	hidea.com AZ Admin 1.0 has news_det.php?cod= SQL Injection.	2019-07-11	7.5	CVE-2019-13507 MISC
hsycms -- hsycms	An issue was discovered in Hsycms V1.1. There is a SQL injection vulnerability via a /news/*.html page.	2019-07-10	7.5	CVE-2019-10653 MISC
oniguruma_project -- oniguruma	A use-after-free in onig_new_deluxe() in regext.c in Oniguruma 6.9.2 allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression. The attacker provides a pair of a	2019-07-10	7.5	CVE-2019-13224 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe(). Oniguruma issues often affect Ruby, as well as common optional libraries for PHP and Rust.			
strong_password_project -- strong_password	The strong_password gem 0.0.7 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party. The current version, without this backdoor, is 0.0.6.	2019-07-08	7.5	CVE-2019-13354 MISC MISC MISC MISC
teclib-edition -- fields	An issue was discovered in the Teclib Fields plugin through 1.9.2 for GLPI. it allows SQL Injection via container_id and old_order parameters to ajax/reorder.php by an unauthenticated user.	2019-07-10	7.5	CVE-2019-12723 MISC MISC CONFIRM
trape_project -- trape	Trape through 2019-05-08 has SQL injection via the data[2] variable in core/db.py, as demonstrated by the /bs t parameter.	2019-07-10	7.5	CVE-2019-13489 MISC
typo3 -- typo3	TYPO3 8.x through 8.7.26 and 9.x through 9.5.7 allows Deserialization of Untrusted Data.	2019-07-09	7.5	CVE-2019-12747 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vivotek -- fd8136_firmware	Vivotek FD8136 devices allow Remote Command Injection, related to BusyBox and wget.	2019-07-10	10.0	CVE-2018-14494 MISC MISC
vivotek -- fd8136_firmware	Vivotek FD8136 devices allow Remote Command Injection, aka "another command injection vulnerability in our target device," a different issue than CVE-2018-14494.	2019-07-10	10.0	CVE-2018-14495 MISC MISC
vivotek -- fd8136_firmware	Vivotek FD8136 devices allow remote memory corruption and remote code execution because of a stack-based buffer overflow, related to sprintf, vlocal_buff_4326, and set_getparam.cgi.	2019-07-10	7.5	CVE-2018-14496 MISC MISC
yoast -- yoast_seo	The Yoast SEO plugin before 11.6-RC5 for WordPress does not properly restrict unfiltered HTML in term descriptions.	2019-07-09	7.5	CVE-2019-13478 MISC

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alsa-project -- alsa	posix/JackSocket.cpp in libjack in JACK2 1.9.1 through 1.9.12 (as distributed with alsa-plugins 1.1.7 and later) has a "double file descriptor close" issue during a failed connection attempt when jackd2 is not running. Exploitation success depends on multithreaded timing of that double close, which can result in unintended information disclosure, crashes, or file corruption due to having the wrong file associated with the file descriptor.	2019-07-05	6.8	CVE-2019-13351 MISC MISC
apachefriends -- xampp	iart.php in XAMPP 1.7.0 has XSS, a related issue to CVE-2008-3569.	2019-07-09	4.3	CVE-2019-8920 BID MISC
cesanta -- mongoose	mq_parse_http in mongoose.c in Mongoose 6.15 has a heap-based buffer over-read.	2019-07-10	5.0	CVE-2019-13503 MISC MISC
cisco -- unified_communications_manager	A vulnerability in the Session Initiation Protocol (SIP) protocol	2019-07-05	5.0	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	implementation of Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient validation of input SIP traffic. An attacker could exploit this vulnerability by sending a malformed SIP packet to an affected Cisco Unified Communications Manager. A successful exploit could allow the attacker to trigger a new registration process on all connected phones, temporarily disrupting service.			1887 CISCO
codedoc_project -- codedoc	Codedoc v3.2 has a stack-based buffer overflow in add_variable in codedoc.c, related to codedoc_strlcpy.	2019-07-06	6.8	CVE-2019-13362 MISC
crudlab -- wp_like_button	An authentication bypass vulnerability in the CRUDLab WP Like Button plugin through	2019-07-05	5.0	CVE-2019-13344 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	1.6.0 for WordPress allows unauthenticated attackers to change settings. The contains() function in wp_like_button.php did not check if the current request is made by an authorized user, thus allowing any unauthenticated user to successfully update settings, as demonstrated by the wp-admin/admin.php?page=facebook-like-button each_page_url or code_snippet parameter.			MISC MISC
custom4web -- wp_open_graph	Cross-site request forgery (CSRF) vulnerability in WP Open Graph 1.6.1 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	CVE-2019-5960 JVN
digisol -- dg-hr-3300_firmware	Digisol Wireless Wifi Home Router HR-3300 allows XSS via the userid or password parameter to the admin login page.	2019-07-05	4.3	CVE-2018-14027 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dlink -- central_wifimanager	A cross-site scripting (XSS) vulnerability in resource view in PayAction.class.php in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 allows remote attackers to inject arbitrary web script or HTML via the index.php/Pay/passcodeAuth passcode parameter.	2019-07-06	4.3	CVE-2019-13374 MISC CONFIRM MISC
dlink -- dir-655_firmware	D-Link DIR-655 C devices before 3.02B05 BETA03 allow remote attackers to force a blank password via the apply_sec.cgi setup_wizard parameter.	2019-07-11	5.0	CVE-2019-13560 MISC MISC MISC
dlink -- dir-655_firmware	D-Link DIR-655 C devices before 3.02B05 BETA03 allow XSS, as demonstrated by the /www/ping_response.cgi ping_ipaddr parameter, the /www/ping6_response.cgi ping6_ipaddr parameter, and the /www/apply_sec.cgi html_response_return_page parameter.	2019-07-11	4.3	CVE-2019-13562 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dlink -- dir-655_firmware	D-Link DIR-655 C devices before 3.02B05 BETA03 allow CSRF for the entire management console.	2019-07-11	6.8	CVE-2019-13563 MISC MISC MISC
dropbox -- dropbox	Dropbox.exe (and QtWebEngineProcess.exe in the Web Helper) in the Dropbox desktop application 71.4.108.0 store cleartext credentials in memory upon successful login or new account creation. These are not securely freed in the running process.	2019-07-08	4.3	CVE-2019-12171 MISC MISC
dwbooster -- appointment_hour_booking	The Appointment Hour Booking plugin 1.1.44 for WordPress allows XSS via the E-mail field, as demonstrated by email_1.	2019-07-11	4.3	CVE-2019-13505 MISC MISC
enhancesoft -- osticket	Unauthenticated Stored XSS in osTicket 1.10.1 allows a remote attacker to gain admin privileges by injecting arbitrary web script or HTML via arbitrary file extension while creating a support ticket.	2019-07-09	4.3	CVE-2019-13397 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/switch.php has an Open Redirect via the current_page parameter.	2019-07-05	5.8	CVE-2018-12621 MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. htdocs/ajax/update.php has XSS via the field_name parameter.	2019-07-10	4.3	CVE-2018-12622 MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. htdocs/switch.php has XSS via the current_page parameter.	2019-07-10	4.3	CVE-2018-12623 MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/validate.php has XSS via the values parameter.	2019-07-10	4.3	CVE-2018-12625 MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/popup.php has XSS via the cat parameter.	2019-07-10	4.3	CVE-2018-12626 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/list.php has XSS via the show_notification_list_issues or show_authorized_issues parameter.	2019-07-10	4.3	CVE-2018-12627 MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. CSRF in htdocs/manage/users.php allows creating another user with admin privileges.	2019-07-10	6.8	CVE-2018-12628 MISC CONFIRM
exiv2 -- exiv2	There is an out-of-bounds read in Exiv2::MrwImage::readMetadata in mrwimage.cpp in Exiv2 through 0.27.2.	2019-07-10	4.3	CVE-2019-13504 BID MISC MISC
ffmpeg -- ffmpeg	In FFmpeg 4.1.3, there is a division by zero at adx_write_trailer in libavformat/rawenc.c. This may be related to two NULL pointers passed as arguments at libavcodec/frame_thread_encoder.c.	2019-07-07	4.3	CVE-2019-13390 BID MISC MISC MISC MISC MISC
fla-shop -- html5_maps	Cross-site request forgery (CSRF)	2019-07-05	6.8	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability in HTML5 Maps 1.6.5.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.			5983 MISC MISC MISC
flarum -- flarum	Flarum before 0.1.0-beta.9 allows CSRF against all POST endpoints, as demonstrated by changing admin settings.	2019-07-07	6.8	CVE-2019-13183 CONFIRM MISC CONFIRM
fortinet -- fcm-mb40_firmware	Dynacolor FCM-MB40 v1.2.0.0 devices have a hard-coded SSL/TLS key that is used during an administrator's SSL conversation.	2019-07-07	4.3	CVE-2019-13399 MISC
fortinet -- fcm-mb40_firmware	Dynacolor FCM-MB40 v1.2.0.0 use /etc/appWeb/appweb.pass to store administrative web-interface credentials in cleartext. These credentials can be retrieved via cgi-bin/getuserinfo.cgi?mode=info.	2019-07-07	5.0	CVE-2019-13400 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fortinet -- fcm-mb40_firmware	Dynacolor FCM-MB40 v1.2.0.0 devices have CSRF in all scripts under cgi-bin/.	2019-07-07	6.8	CVE-2019-13401 MISC
fortinet -- fcm-mb40_firmware	/usr/sbin/default.sh and /usr/apache/htdocs/cgi-bin/admin/hardfactorydefault.cgi on Dynacolor FCM-MB40 v1.2.0.0 devices implement an incomplete factory-reset process. A backdoor can persist because neither system accounts nor the set of services is reset.	2019-07-07	6.5	CVE-2019-13402 MISC
gitea -- gitea	Gitea 1.7.2, 1.7.3 is affected by: Cross Site Scripting (XSS). The impact is: execute JavaScript in victim's browser, when the vulnerable repo page is loaded. The component is: repository's description. The attack vector is: victim must navigate to public and affected repo page.	2019-07-11	4.3	CVE-2019-1010314 MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition 11.x before 11.3.11, 11.4.x	2019-07-10	4.3	CVE-2018-19493 BID CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	before 11.4.8, and 11.5.x before 11.5.1. There is a persistent XSS vulnerability in the environment pages due to a lack of input validation and output encoding.			RM MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition 11.x before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is an incorrect access vulnerability that allows an unauthorized user to view private group names.	2019-07-10	4.0	CVE-2018-19494 CONFIRM MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is an SSRF vulnerability in the Prometheus integration.	2019-07-10	4.0	CVE-2018-19495 CONFIRM MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and	2019-07-10	4.0	CVE-2018-19496

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Enterprise Edition 10.x and 11.x before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is an incorrect access control vulnerability that permits a user with insufficient privileges to promote a project milestone to a group milestone.			CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.8 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an authorization vulnerability that allows access to the web-UI as a user using a Personal Access Token of any scope.	2019-07-10	6.5	CVE-2018-19569 BID CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.18 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an SSRF vulnerability in webhooks.	2019-07-10	4.0	CVE-2018-19571 MISC MISC
gitlab -- gitlab	GitLab CE 8.17 and later and EE 8.3 and	2019-07-10	4.3	CVE-2018-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	later have a symlink time-of-check-to-time-of-use race condition that would allow unauthorized access to files in the GitLab Pages chroot environment. This is fixed in versions 11.5.1, 11.4.8, and 11.3.11.			19572 CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 10.1 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an insecure direct object reference issue that allows a user to make comments on a locked issue.	2019-07-10	4.0	CVE-2018-19575 BID CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.6 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an access control issue that allows a Guest user to make changes to or delete their own comments on an issue, after the issue was made Confidential.	2019-07-10	6.4	CVE-2018-19576 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gitlab -- gitlab	Gitlab CE/EE, versions 8.6 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an incorrect access control vulnerability that displays to an unauthorized user the title and namespace of a confidential issue.	2019-07-10	5.0	CVE-2018-19577 CONFIRM MISC
gitlab -- gitlab	GitLab EE, version 11.5 before 11.5.1, is vulnerable to an insecure object reference issue that permits a user with Reporter privileges to view the Jaeger Tracing Operations page.	2019-07-10	4.0	CVE-2018-19578 CONFIRM MISC
gitlab -- gitlab	All versions of GitLab prior to 11.5.1, 11.4.8, and 11.3.11 do not send an email to the old email address when an email address change is made.	2019-07-10	5.0	CVE-2018-19580 CONFIRM MISC
gitlab -- gitlab	GitLab EE, versions 8.3 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, is vulnerable to an insecure object reference vulnerability	2019-07-10	5.0	CVE-2018-19581 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	that allows a Guest user to set the weight of an issue they create.			
gitlab -- gitlab	GitLab EE, versions 11.4 before 11.4.8 and 11.5 before 11.5.1, is affected by an insecure direct object reference vulnerability that permits an unauthorized user to publish the draft merge request comments of another user.	2019-07-10	4.0	CVE-2018-19582 CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.0 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, would log access tokens in the Workhorse logs, permitting administrators with access to the logs to see another user's token.	2019-07-10	4.0	CVE-2018-19583 CONFIRM MISC
gitlab -- gitlab	GitLab EE, versions 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, is vulnerable to an insecure direct object reference vulnerability that allows authenticated, but	2019-07-10	5.0	CVE-2018-19584 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthorized, users to view members and milestone details of private groups.			
google -- android	In FileInputStream::Read of file_input_stream.cc, there is a possible memory corruption due to uninitialized data. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-116114182.	2019-07-08	6.8	CVE-2019-2105 CONFIRM
google -- android	In save_attr_seq of sdp_discovery.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not	2019-07-08	5.0	CVE-2019-2116 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-117105007.			
helpy.io -- helpy	Helpy before 2.2.0 allows agents to edit admins.	2019-07-10	6.5	CVE-2018-20851 MISC MISC
ibm -- cloud_application_performance_management	IBM Application Performance Management (IBM Monitoring 8.1.4) could allow a remote attacker to induce the application to perform server-side DNS lookups of arbitrary domain names. IBM X-Force ID: 158270.	2019-07-11	5.0	CVE-2019-4131 XF CONFIRM
ibm -- jazz_for_service_management	IBM Jazz for Service Management 1.1.3 and 1.1.3.2 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs,	2019-07-11	5.0	CVE-2019-4193 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	referrer header or browser history. IBM X-force ID: 159032.			
idoors -- idoors_reader	iDoors Reader 2.10.17 and earlier allows an attacker on the same network segment to bypass authentication to access the management console and operate the product via unspecified vectors.	2019-07-05	5.8	CVE-2019-5964 MISC MISC
ignitedcms_project -- ignitedcms	index.php/admin/permissions in Ignited CMS through 2017-02-19 allows CSRF to add an administrator.	2019-07-06	6.8	CVE-2019-13370 MISC
imagemagick -- imagemagick	In ImageMagick 7.0.8-50 Q16, ComplexImages in MagickCore/fourier.c has a heap-based buffer over-read because of incorrect calls to GetCacheViewVirtualPixels.	2019-07-07	6.8	CVE-2019-13391 MISC MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-54 Q16 allows Division by Zero in RemoveDuplicateLayers in MagickCore/layer.c.	2019-07-09	4.3	CVE-2019-13454 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
intersystems -- cache	Intersystems Cache 2017.2.2.865.0 allows XSS.	2019-07-11	4.3	CVE-2018-17150 MISC
intersystems -- cache	Intersystems Cache 2017.2.2.865.0 has Incorrect Access Control.	2019-07-11	5.5	CVE-2018-17151 MISC
intersystems -- cache	Intersystems Cache 2017.2.2.865.0 allows XXE.	2019-07-11	5.5	CVE-2018-17152 MISC
invoxia -- nvx220_firmware	Invoxia NVX220 devices allow access to /bin/sh via escape from a restricted CLI, leading to disclosure of password hashes.	2019-07-05	5.0	CVE-2018-14529 MISC
joruri -- joruri_cms_2017	Cross-site scripting vulnerability in Joruri CMS 2017 Release2 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	4.3	CVE-2019-5967 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
joruri -- joruri_mail	Open redirect vulnerability in Joruri Mail 2.1.4 and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2019-07-05	5.8	CVE-2019-5965 MISC MISC
joruri -- joruri_mail	Joruri Mail 2.1.4 and earlier does not properly manage sessions, which allows remote attackers to impersonate an arbitrary user and alter/disclose the information via unspecified vectors.	2019-07-05	5.8	CVE-2019-5966 MISC MISC
keynto -- team_password_manager	KEYNTO Team Password Manager 1.5.0 allows XSS because data saved from websites is mishandled in the online vault.	2019-07-09	4.3	CVE-2019-13380 FULL DISC
libpng -- libpng	An issue has been found in third-party PNM decoding associated with libpng 1.6.35. It is a stack-based buffer overflow in the function get_token in	2019-07-10	6.8	CVE-2018-14550 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	pnm2png.c in pnm2png.			
mailvelope -- mailvelope	Mailvelope prior to 3.1.0 is vulnerable to a clickjacking attack against the settings page. As the settings page is intended to be accessible from web applications, the browser's extension isolation mechanisms are disabled (web_accessible_resources). Mailvelope implements additional measures to prevent web applications from directly embedding the settings page, but this mechanism can be bypassed.	2019-07-09	4.3	CVE-2019-9147 CONFIRM
mailvelope -- mailvelope	Mailvelope prior to 3.3.0 accepts or operates with invalid PGP public keys: Mailvelope allows importing keys that contain users without a valid self-certification. Keys that are obviously invalid are not rejected during import. An attacker that is able to get a victim to import a manipulated key could	2019-07-09	4.3	CVE-2019-9148 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	claim to have signed a message that originates from another person.			
mailvelope -- mailvelope	Mailvelope prior to 3.3.0 allows private key operations without user interaction via its client-API. By modifying an URL parameter in Mailvelope, an attacker is able to sign (and encrypt) arbitrary messages with Mailvelope, assuming the private key password is cached. A second vulnerability allows an attacker to decrypt an arbitrary message when the GnuPG backend is used in Mailvelope.	2019-07-09	6.4	CVE-2019-9149 CONFIRM
mailvelope -- mailvelope	Mailvelope prior to 3.3.0 does not require user interaction to import public keys shown on web page. This functionality can be tricked to either hide a key import from the user or obscure which key was imported.	2019-07-09	5.0	CVE-2019-9150 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mastodon-tootdon -- tootdon_for_mastodon	The Android App 'Tootdon for Mastodon' version 3.4.1 and earlier does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2019-07-05	5.8	CVE-2019-5961 MISC MISC
mediawiki -- mediawiki	Wikimedia MediaWiki through 1.32.1 allows CSRF.	2019-07-10	6.8	CVE-2019-12466 CONFIRM MISC BUGTRAQ DEBIAN
mediawiki -- mediawiki	Wikimedia MediaWiki 1.23.0 through 1.32.1 has an information leak. Privileged API responses that include whether a recent change has been patrolled may be cached publicly. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	5.0	CVE-2019-12474 CONFIRM MISC BUGTRAQ DEBIAN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
odoo -- odoo	The Odoo Community Association (OCA) dbfilter_from_header module makes Odoo 8.x, 9.x, 10.x, and 11.x vulnerable to ReDoS (regular expression denial of service) under certain circumstances.	2019-07-05	5.0	CVE-2018-14733 CONFIRM MISC MISC MISC MISC
oniguruma_project -- oniguruma	A NULL Pointer Dereference in match_at() in regexec.c in Oniguruma 6.9.2 allows attackers to potentially cause denial of service by providing a crafted regular expression. Oniguruma issues often affect Ruby, as well as common optional libraries for PHP and Rust.	2019-07-10	5.0	CVE-2019-13225 CONFIRM
opencats -- opencats	lib/DocumentToText.php in OpenCats before 0.9.4-3 has XXE that allows remote users to read files on the underlying operating system. The attacker must upload a file in the docx or odt format.	2019-07-05	4.3	CVE-2019-13358 MISC MISC MISC
otrs -- otrs	An issue was discovered in Open	2019-07-08	4.9	CVE-2018-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Ticket Request System (OTRS) 6.0.x through 6.0.7. A carefully constructed email could be used to inject and execute arbitrary stylesheet or JavaScript code in a logged in customer's browser in the context of the OTRS customer panel application.			11563 CONFIRM CONFIRM MISC
paypal -- adaptive_payments_sdk	paypal/adaptivepayments-sdk-php v3.9.2 is vulnerable to a reflected XSS in the SetPaymentOptions.php resulting code execution	2019-07-10	4.3	CVE-2017-6217 MISC
phpwind -- phpwind	PHPWind 9.1.0 has XSS vulnerabilities in the c and m parameters of the index.php file.	2019-07-09	4.3	CVE-2019-13472 MISC
pingidentity -- agentless_integration_kit	XSS exists in Ping Identity Agentless Integration Kit before 1.5.	2019-07-11	4.3	CVE-2019-13564 CONFIRM
pyxtrlock_project -- pyxtrlock	pyxtrlock 0.3 and earlier is affected by: Incorrect Access Control. The impact is:	2019-07-11	4.6	CVE-2019-101031

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	False locking impression when run in a non-X11 session. The fixed version is: 0.4.			6 MISC
sap -- information_steward	SAP Information Steward, version 4.2, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-07-10	4.3	CVE-2019-0329 BID MISC CONFIRM
sony -- vaio_update	Improper authorization vulnerability in VAIO Update 7.3.0.03150 and earlier allows an attackers to execute arbitrary executable file with administrative privilege via unspecified vectors.	2019-07-05	6.8	CVE-2019-5981 MISC MISC
sony -- vaio_update	Improper download file verification vulnerability in VAIO Update 7.3.0.03150 and earlier allows remote attackers to conduct a man-in-the-middle attack via a malicous wireless LAN access point. A successful exploitation may result in a malicious file being downloaded/executed.	2019-07-05	5.4	CVE-2019-5982 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
squid-cache -- squid	The cachemgr.cgi web module of Squid through 4.7 has XSS via the user_name or auth parameter.	2019-07-05	4.3	CVE-2019-13345 MISC MISC MLIST
sukimalab -- attendance_manager	Cross-site scripting vulnerability in Attendance Manager 0.5.6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	4.3	CVE-2019-5970 MISC MISC MISC MISC
sukimalab -- attendance_manager	Cross-site request forgery (CSRF) vulnerability in Attendance Manager 0.5.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	CVE-2019-5971 MISC MISC MISC MISC
sukimalab -- online_lesson_booking	Cross-site scripting vulnerability in Online Lesson Booking 0.8.6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	4.3	CVE-2019-5972 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
teclib-edition -- fields	An issue was discovered in the Teclib News plugin through 1.5.2 for GLPI. It allows a stored XSS attack via the $_POST['name'] parameter.	2019-07-10	4.3	CVE-2019-12724 MISC MISC CONFIRM
trape_project -- trape	A cross-site scripting (XSS) vulnerability in static/js/trape.js in Trape through 2019-05-08 allows remote attackers to inject arbitrary web script or HTML via the country, query, or refer parameter to the /register URI, because the jQuery prepend() method is used.	2019-07-10	4.3	CVE-2019-13488 MISC
typo3 -- typo3	TYPO3 8.3.0 through 8.7.26 and 9.0.0 through 9.5.7 allows XSS.	2019-07-09	4.3	CVE-2019-12748 CONFIRM
waspthemes -- custom_css_pro	Cross-site request forgery (CSRF) vulnerability in Custom CSS Pro 1.0.3 and earlier allows remote attackers to hijack the authentication of	2019-07-05	6.8	CVE-2019-5984 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	administrators via unspecified vectors.			
weseek -- growi	Cross-site request forgery (CSRF) vulnerability in GROWI v3.4.6 and earlier allows remote attackers to hijack the authentication of administrators via updating user's 'Basic Info'.	2019-07-05	6.8	CVE-2019-5968 MISC MISC
weseek -- growi	Open redirect vulnerability in GROWI v3.4.6 and earlier allows remote attackersto redirect users to arbitrary web sites and conduct phishing attacks via the process of login.	2019-07-05	5.8	CVE-2019-5969 MISC MISC
wikindx_project -- wikindx	A cross-site scripting (XSS) vulnerability in noMenu() and noSubMenu() in core/navigation/MENU.php in WIKINDX prior to version 5.8.1 allows remote attackers to inject arbitrary web script or HTML via the method parameter.	2019-07-08	4.3	CVE-2019-12930 CONFIRM CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zoho -- salesiq	Cross-site scripting vulnerability in Zoho SalesIQ 1.0.8 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	4.3	CVE-2019-5962 MISC MISC
zoho -- salesiq	Cross-site request forgery (CSRF) vulnerability in Zoho SalesIQ 1.0.8 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	CVE-2019-5963 MISC MISC
zohocorp -- manageengine_assetexplorer	An issue was discovered in Zoho ManageEngine AssetExplorer. There is XSS via the RCSettings.do rdsName parameter.	2019-07-11	4.3	CVE-2019-12595 MISC MISC
zohocorp -- manageengine_assetexplorer	An issue was discovered in Zoho ManageEngine AssetExplorer. There is XSS via SoftwareListView.do with the parameter swType or swComplianceType.	2019-07-11	4.3	CVE-2019-12596 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zohocorp -- manageengine_assetexplorer	An issue was discovered in Zoho ManageEngine AssetExplorer. There is XSS via ResourcesAttachments.jsp with the parameter pageName.	2019-07-11	4.3	CVE-2019-12597 MISC MISC
zohocorp -- manageengine_servicedesk_plus	An issue was discovered in the Purchase component of Zoho ManageEngine ServiceDesk Plus. There is XSS via the SearchN.do search field, a different vulnerability than CVE-2019-12189.	2019-07-11	4.3	CVE-2019-12539 MISC MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/page-edit.php (content box), which can be used to get a user's cookie.	2019-07-05	3.5	CVE-2019-13339 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/post-edit.php via the content box. An attacker can use it to get a user's cookie. This is different from CVE-2018-10296, CVE-2018-16233, CVE-2018-20520, and CVE-2019-13186.	2019-07-05	3.5	CVE-2019-13340 MISC
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/conf.php (comment box), which can be used to get a user's cookie.	2019-07-05	3.5	CVE-2019-13341 MISC
cyberpowersystems -- powerpanel	A stored XSS vulnerability in the Agent/Center component of CyberPower PowerPanel Business Edition 3.4.0 allows a privileged attacker to embed malicious JavaScript in the SNMP trap receivers form. Upon visiting the /agent/action_recipient Event Action/Recipient page, the embedded code will be executed in the browser of the victim.	2019-07-09	3.5	CVE-2019-13070 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gitlab -- gitlab	GitLab CE/EE, versions 11.3 before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an XSS vulnerability in Markdown fields via unrecognized HTML tags.	2019-07-10	3.5	CVE-2018-19570 CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 10.3 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an XSS vulnerability in Markdown fields via Mermaid.	2019-07-10	3.5	CVE-2018-19573 CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 7.6 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an XSS vulnerability in the OAuth authorization page.	2019-07-10	3.5	CVE-2018-19574 MISC MISC
gitlab -- gitlab	GitLab EE version 11.5 is vulnerable to a persistent XSS vulnerability in the Operations page. This is fixed in 11.5.1.	2019-07-10	3.5	CVE-2018-19579 CONFIRM MISC
google -- android	In HIDL, safe_union, and other C++ structs/unions being sent	2019-07-08	2.1	CVE-2019-2104 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to application processes, there are uninitialized fields. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-131356202			
google -- android	In setup wizard there is a bypass of some checks when wifi connection is skipped. This could lead to factory reset protection bypass with no additional privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-122597079.	2019-07-08	2.1	CVE-2019-2113 CONFIRM
google -- android	In checkQueryPermission of TelephonyProvider.java, there is a possible disclosure of secure data due to a missing permission check. This could lead to local information disclosure about carrier systems	2019-07-08	2.1	CVE-2019-2117 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-124107808.			
google -- android	In various functions of Parcel.cpp, there are uninitialized or partially initialized stack variables. These could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-130161842.	2019-07-08	2.1	CVE-2019-2118 CONFIRM
google -- android	In multiple functions of key_store_service.cpp, there is a possible Information Disclosure due to improper locking. This could lead to local information disclosure of protected data with no additional execution privileges needed. User interaction is not needed	2019-07-08	2.1	CVE-2019-2119 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-131622568.			
ibm -- multicloud_manager	IBM Multicloud Manager 3.1.0, 3.1.1, and 3.1.2 ibm-mcm-chart could allow a local attacker with admin privileges to obtain highly sensitive information upon deployment. IBM X-Force ID: 158144.	2019-07-11	2.1	CVE-2019-4118 CONFIRM XF
libosinfo -- libosinfo	libosinfo 1.5.0 allows local users to discover credentials by listing a process, because credentials are passed to osinfo-install-script via the command line.	2019-07-05	2.1	CVE-2019-13313 MLIST MISC MISC MISC MISC
nagios -- nagios_xi	Nagios XI before 5.5.4 has XSS in the auto login admin management page.	2019-07-10	3.5	CVE-2018-17147 BID MISC
redhat -- virt-bootstrap	virt-bootstrap 1.1.0 allows local users to discover a root password by listing a process, because this	2019-07-05	2.1	CVE-2019-13314 MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	password may be present in the --root-password option to virt_bootstrap.py.			MISC MISC

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alarm.com -- adc-v522ir_devices	Alarm.com ADC-V522IR 0100b9 devices have Incorrect Access Control, a different issue than CVE-2018-19588. This occurs because of incorrect protection of VPN certificates (used for initiating a VPN session to the Alarm.com infrastructure) on the local camera device.	2019-07-11	not yet calculated	CVE-2019-9657 MISC
alarm.com -- adc-v522ir_devices	Alarm.com ADC-V522IR 0100b9 devices have Incorrect Access Control.	2019-07-11	not yet calculated	CVE-2018-19588 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- kafka	In Apache Kafka versions between 0.11.0.0 and 2.1.0, it is possible to manually craft a Produce request which bypasses transaction/idempotent ACL validation. Only authenticated clients with Write permission on the respective topics are able to exploit this vulnerability. Users should upgrade to 2.1.1 or later where this vulnerability has been fixed.	2019-07-11	not yet calculated	CVE-2018-17196 MISC
apple -- macos	hide.me before 2.4.4 on macOS suffers from a privilege escalation vulnerability in the connectWithExecutablePath:configFilePath:configFileName method of the me_hide_vpnhelper.Helper class in the me.hide.vpnhelper macOS privilege helper tool. This method takes user-supplied input and can be used to escalate privileges, as well as obtain the ability to run any application on the system in the root context.	2019-07-08	not yet calculated	CVE-2019-12174 MISC
arlo -- basestation	Arlo Basestation firmware 1.12.0.1_27940 and prior contain a hardcoded username and password combination that allows root access to the device when an onboard serial interface is connected to.	2019-07-09	not yet calculated	CVE-2019-3950 CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				NFIRM
arlo -- basestation	Arlo Basestation firmware 1.12.0.1_27940 and prior firmware contain a networking misconfiguration that allows access to restricted network interfaces. This could allow an attacker to upload or download arbitrary files and possibly execute malicious code on the device.	2019-07-09	not yet calculated	CVE-2019-3949 CONFIRM
avaya -- control_manager	A SQL injection vulnerability in the reporting component of Avaya Control Manager could allow an unauthenticated attacker to execute arbitrary SQL commands and retrieve sensitive data related to other users on the system. Affected versions of Avaya Control Manager include 7.x and 8.0.x versions prior to 8.0.4.0. Unsupported versions not listed here were not evaluated.	2019-07-11	not yet calculated	CVE-2019-7003 BID CONFIRM
avtech -- room_alert_3e	On AVTECH Room Alert 3E devices before 2.2.5, an attacker with access to the device's web interface may escalate privileges from an unauthenticated user to administrator by performing a cmd.cgi?action=ResetDefaults&	2019-07-07	not yet calculated	CVE-2019-13379 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	src=RA reset and using the default credentials to get in.			CMISC
bks -- bks_ebk_ethernet-buskoppler_pro	BKS EBK Ethernet-Buskoppler Pro before 3.01 allows Unrestricted Upload of a File with a Dangerous Type.	2019-07-05	not yet calculated	CVE-2019-12971 MISC
blackberry -- qnx_software_development_platform	An information disclosure vulnerability leading to a potential local escalation of privilege in the procfs service (the /proc filesystem) of BlackBerry QNX Software Development Platform version(s) 6.5.0 SP1 and earlier could allow an attacker to potentially gain unauthorized access to a chosen process address space.	2019-07-12	not yet calculated	CVE-2019-8998 MISC
broadlearning -- eclass	Any URLs with download_attachment.php under templates or home folders can allow arbitrary files downloaded without login in BroadLearning eClass before version ip.2.5.10.2.1.	2019-07-11	not yet calculated	CVE-2019-9886 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM CONFIRM
castle_rock_computing -- snmpc	nodeimp.exe in Castle Rock SNMPc before 9.0.12.1 and 10.x before 10.0.9 has a stack-based buffer overflow via a long variable string in a Map Objects text file.	2019-07-12	not yet calculated	CVE-2019-13494 MISC MISC
cisco -- adaptive_security_appliance_software_and_firepower_threat_defense_software	A vulnerability in the cryptographic driver for Cisco Adaptive Security Appliance Software (ASA) and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reboot unexpectedly. The vulnerability is due to incomplete input validation of a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) ingress packet header. An attacker could exploit this vulnerability by sending a crafted TLS/SSL packet to an interface on the targeted device. An exploit could allow the	2019-07-10	not yet calculated	CVE-2019-1873 BID CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to cause the device to reload, which will result in a denial of service (DoS) condition. Note: Only traffic directed to the affected system can be used to exploit this vulnerability. This vulnerability affects systems configured in routed and transparent firewall mode and in single or multiple context mode. This vulnerability can be triggered by IPv4 and IPv6 traffic. A valid SSL or TLS session is required to exploit this vulnerability.			
cisco -- advanced_malware_protection_for_endpoints_for_windows	A vulnerability in Cisco Advanced Malware Protection (AMP) for Endpoints for Windows could allow an authenticated, local attacker with administrator privileges to execute arbitrary code. The vulnerability is due to insufficient validation of dynamically loaded modules. An attacker could exploit this vulnerability by placing a file in a specific location in the Windows filesystem. A successful exploit could allow the attacker to execute the code with the privileges of the AMP service.	2019-07-05	not yet calculated	CVE-2019-1932 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- email_security_appliance	A vulnerability in the attachment scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured content filters on the device. The vulnerability is due to improper input validation of the email body. An attacker could exploit this vulnerability by naming a malicious attachment with a specific pattern. A successful exploit could allow the attacker to bypass configured content filters that would normally block the attachment.	2019-07-05	not yet calculated	CVE-2019-1921 CISCO
cisco -- email_security_appliance	A vulnerability in the email message scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured filters on the device. The vulnerability is due to improper input validation of certain email fields. An attacker could exploit this vulnerability by sending a crafted email message to a recipient protected by the ESA. A successful exploit could allow the attacker to bypass configured message filters and inject arbitrary	2019-07-05	not yet calculated	CVE-2019-1933 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	scripting code inside the email body. The malicious code is not executed by default unless the recipient's email client is configured to execute scripts contained in emails.			
cisco -- enterprise_nfv_infrastructure_software	A vulnerability in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, remote attacker with administrator privileges to overwrite or read arbitrary files on the underlying operating system (OS) of an affected device. The vulnerability is due to improper input validation in NFVIS filesystem commands. An attacker could exploit this vulnerability by using crafted variables during the execution of an affected command. A successful exploit could allow the attacker to overwrite or read arbitrary files on the underlying OS.	2019-07-05	not yet calculated	CVE-2019-1894 CISCO
cisco -- enterprise_nfv_infrastructure_software	A vulnerability in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device as root. The vulnerability	2019-07-05	not yet calculated	CVE-2019-1893 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	is due to insufficient input validation of a configuration file that is accessible to a local shell user. An attacker could exploit this vulnerability by including malicious input during the execution of this file. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS as root.			
cisco -- firepower_management_center	Multiple vulnerabilities in the RSS dashboard in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2019-07-05	not yet calculated	CVE-2019-1931 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- firepower_management_center	Multiple vulnerabilities in the RSS dashboard in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2019-07-05	not yet calculated	CVE-2019-1930 CISCO
cisco -- ios_xr_software	A vulnerability in the implementation of Border Gateway Protocol (BGP) functionality in Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to incorrect processing of certain BGP update messages. An	2019-07-05	not yet calculated	CVE-2019-1909 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker could exploit this vulnerability by sending BGP update messages that include a specific set of attributes to be processed by an affected system. A successful exploit could allow the attacker to cause the BGP process to restart unexpectedly, resulting in a DoS condition. The Cisco implementation of BGP accepts incoming BGP traffic from explicitly defined peers only. To exploit this vulnerability, the malicious BGP update message would need to come from a configured, valid BGP peer or would need to be injected by the attacker into the victim's BGP network on an existing, valid TCP connection to a BGP peer.			
cisco -- ip_phone_7800_series_and_8800_series	A vulnerability in Cisco SIP IP Phone Software for Cisco IP Phone 7800 Series and 8800 Series could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected phone. The vulnerability is due to insufficient validation of input Session Initiation Protocol (SIP) packets. An attacker could exploit this vulnerability by altering the SIP replies that are sent to the affected phone during	2019-07-05	not yet calculated	CVE-2019-1922 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the registration process. A successful exploit could allow the attacker to cause the phone to reboot and not complete the registration process.			
cisco -- small_business_200_and_300_and_500_series_managed_switches	A vulnerability in the Secure Sockets Layer (SSL) input packet processor of Cisco Small Business 200, 300, and 500 Series Managed Switches could allow an unauthenticated, remote attacker to cause a memory corruption on an affected device. The vulnerability is due to improper validation of HTTPS packets. An attacker could exploit this vulnerability by sending a malformed HTTPS packet to the management web interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a denial of service (DoS) condition.	2019-07-05	not yet calculated	CVE-2019-1892 CISCO
cisco -- small_business_200_and_300_and_500_series_managed_switches	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper	2019-07-05	not yet calculated	CVE-2019-1891 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.			
cisco -- unified_communications_domain_manager	A vulnerability in the CLI of Cisco Unified Communications Domain Manager (Cisco Unified CDM) Software could allow an authenticated, local attacker to escape the restricted shell. The vulnerability is due to insufficient input validation of shell commands. An attacker could exploit this vulnerability by executing crafted commands in the shell. A successful exploit could allow the attacker to escape the restricted shell and access commands in the context of the restricted shell user, which does not have root privileges.	2019-07-05	not yet calculated	CVE-2019-1911 CISCO
citrix -- xenserver	The Windows Guest Tools in Citrix XenServer 6.2 SP1 and earlier allows remote attackers to cause a denial of service (guest OS crash) via a crafted Ethernet frame.	2019-07-11	not yet calculated	CVE-2014-3798

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				SECUNIA CONFIRM BID SECTRACK
cloud_foundry -- uaa	Cloud Foundry UAA version prior to 73.3.0, contain endpoints that contains improper escaping. An authenticated malicious user with basic read privileges for one identity zone can extend those reading privileges to all other identity zones and obtain private information on users, clients, and groups in all other identity zones.	2019-07-11	not yet calculated	CVE-2019-11268 CONFIRM
cloudera -- cloudera_manager	Cloudera Manager through 5.15 has Incorrect Access Control.	2019-07-11	not yet calculated	CVE-2018-11744 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cohesity -- dataplatform	A man-in-the-middle vulnerability related to vCenter access was found in Cohesity DataPlatform version 5.x and 6.x prior to 6.1.1c. Cohesity clusters did not verify TLS certificates presented by vCenter. This vulnerability could expose Cohesity user credentials configured to access vCenter.	2019-07-12	not yet calculated	CVE-2019-11242 CONFIRM
container_build_system -- osbs-client	A flaw was found in the yaml.load() function in the osbs-client versions since 0.46 before 0.56.1. Insecure use of the yaml.load() function allowed the user to load any suspicious object for code execution via the parsing of malicious YAML files.	2019-07-11	not yet calculated	CVE-2019-10135 CONFIRM CONFIRM
cyberpower -- powerpanel_business	CSRF in the Agent/Center component of CyberPower PowerPanel Business Edition 3.4.0 allows an attacker to submit POST requests to any forms in the web application. This can be exploited by tricking an authenticated user into visiting an attacker controlled web page.	2019-07-10	not yet calculated	CVE-2019-13071 MISC FULL

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				DISC
damicms -- damicms	An arbitrary file read vulnerability in DamiCMS v6.0.0 allows remote authenticated administrators to read any files in the server via a crafted /admin.php?s=Tpl/Add/id/ URI.	2019-07-10	not yet calculated	CVE-2018-14831 MISC
ddrt -- dashcom_live	Lack of authentication in file-viewing components in DDRT Dashcom Live 2019-05-09 allows anyone to remotely access all claim details by visiting easily guessable dashboard/uploads/claim_files/claim_id_ URLs.	2019-07-09	not yet calculated	CVE-2019-11020 MISC MISC
ddrt -- dashcom_live	Lack of authentication in case-exporting components in DDRT Dashcom Live through 2019-05-08 allows anyone to remotely access all claim details by visiting easily guessable exportpdf/all_claim_detail.php?claim_id= URLs.	2019-07-09	not yet calculated	CVE-2019-11019 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
debian -- mediawiki	An Incorrect Access Control vulnerability was found in Wikimedia MediaWiki 1.18.0 through 1.32.1. It is possible to bypass the limits on IP range blocks ($wgBlockCIDRLimit) by using the API. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	CVE-2019-12472 CONFIRM MISC
debian -- mediawiki	An Incorrect Access Control vulnerability was found in Wikimedia MediaWiki 1.27.0 through 1.32.1. Directly POSTing to Special:ChangeEmail would allow for bypassing re-authentication, allowing for potential account takeover.	2019-07-10	not yet calculated	CVE-2019-12468 MISC CONFIRM MISC BUGTRAQ DEBIAN
debian -- mediawiki	MediaWiki through 1.32.1 has Incorrect Access Control (issue 1 of 3). A spammer can use	2019-	not yet cal	CVE-201

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Special:ChangeEmail to send out spam with no rate limiting or ability to block them. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	07-10	culated	9-12467 CONFIRM MISC BUGTRAQ DEBIAN
debian -- mediawiki	Wikimedia MediaWiki 1.30.0 through 1.32.1 has XSS. Loading user JavaScript from a non-existent account allows anyone to create the account, and perform XSS on users loading that script. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	CVE-2019-12471 CONFIRM MISC BUGTRAQ DEBIAN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
debian -- mediawiki	Wikimedia MediaWiki 1.27.0 through 1.32.1 might allow DoS. Passing invalid titles to the API could cause a DoS by querying the entire watchlist table. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	CVE-2019-12473 CONFIRM MISC BUGTRAQ DEBIAN
debian -- mediawiki	Wikimedia MediaWiki through 1.32.1 has Incorrect Access Control. Suppressed log in RevisionDelete page is exposed. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	CVE-2019-12470 CONFIRM MISC BUGTRAQ DE

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				BIAN
debian -- mediawiki	MediaWiki through 1.32.1 has Incorrect Access Control. Suppressed username or log in Special:EditTags are exposed. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	CVE-2019-12469 CONFIRM MISC BUGTRAQ DEBIAN
debian -- redis	A stack-buffer overflow vulnerability was found in the Redis hyperloglog data structure versions 3.x before 3.2.13, 4.x before 4.0.14 and 5.x before 5.0.4. By corrupting a hyperloglog using the SETRANGE command, an attacker could cause Redis to perform controlled increments of up to 12 bytes past the end of a stack-allocated buffer.	2019-07-11	not yet calculated	CVE-2019-10193 CONFIRM MISC MISC MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CBUGTRAQ DEBIAN
debian -- redis	A heap-buffer overflow vulnerability was found in the Redis hyperloglog data structure versions 3.x before 3.2.13, 4.x before 4.0.14 and 5.x before 5.0.4. By carefully corrupting a hyperloglog using the SETRANGE command, an attacker could trick Redis interpretation of dense HLL encoding to write up to 3 bytes beyond the end of a heap-allocated buffer.	2019-07-11	not yet calculated	CVE-2019-10192 CONFIRM MISC MISC MISC BUGTRAQ DEBIAN
digium -- asterisk	Buffer overflow in res_pjsip_messaging in Digium Asterisk versions 13.21-cert3, 13.27.0, 15.7.2, 16.4.0 and	2019-07-12	not yet calcul	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	earlier allows remote authenticated users to crash Asterisk by sending a specially crafted SIP MESSAGE message.		ated	12827 CONFIRM CONFIRM
digium -- asterisk	An issue was discovered in Asterisk Open Source through 13.27.0, 14.x and 15.x through 15.7.2, and 16.x through 16.4.0, and Certified Asterisk through 13.21-cert3. A pointer dereference in chan_sip while handling SDP negotiation allows an attacker to crash Asterisk when handling an SDP answer to an outgoing T.38 re-invite. To exploit this vulnerability an attacker must cause the chan_sip module to send a T.38 re-invite request to them. Upon receipt, the attacker must send an SDP answer containing both a T.38 UDPTL stream and another media stream containing only a codec (which is not permitted according to the chan_sip configuration).	2019-07-12	not yet calculated	CVE-2019-13161 CONFIRM CONFIRM
e107 -- e107	In e107 v2.1.7, output without filtering results in XSS.	2019-	not yet cal	CVE-201

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
		07-10	culated	8-11734 MISC
eq-3 -- homematic_ccu2_devices	eQ-3 HomeMatic CCU2 devices before 2.41.9 and CCU3 devices before 3.43.16 have buffer overflows in the ReGa ise GmbH HTTP-Server 2.0 component, aka HMCCU-179. This may lead to remote code execution.	2019-07-10	not yet calculated	CVE-2019-10122 MISC MISC
eq-3 -- homematic_ccu2_devices	eQ-3 HomeMatic CCU2 devices before 2.41.8 and CCU3 devices before 3.43.16 use session IDs for authentication but lack authorization checks. An attacker can obtain a session ID via an invalid login attempt to the RemoteApi account, aka HMCCU-154. This leads to automatic login as admin.	2019-07-10	not yet calculated	CVE-2019-10119 MISC MISC
eq-3 -- homematic_ccu2_devices	On eQ-3 HomeMatic CCU2 devices before 2.41.8 and CCU3 devices before 3.43.16, automatic login configuration (aka setAutoLogin) can be achieved by continuing to use a	2019-07-10	not yet calculated	CVE-2019-10120 MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	session ID after a logout, aka HMCCU-154.			CMISC
eq-3 -- homematic_ccu2_devices	eQ-3 HomeMatic CCU2 devices before 2.41.8 and CCU3 devices before 3.43.15 use session IDs for authentication but lack authorization checks. An attacker can obtain a session ID via the user authentication dialogue, aka HMCCU-153. This leads to automatic login as admin.	2019-07-10	not yet calculated	CVE-2019-10121 MISC MISC MISC
fasterxml -- jackson-databind	An issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.5. Use of Jackson default typing along with a gadget class from iBatis allows exfiltration of content. Fixed in 2.7.9.4, 2.8.11.2, and 2.9.6.	2019-07-09	not yet calculated	CVE-2018-11307 CONFIRM MISC MISC MISC
field_test_gem_for_ruby_on_rails --	The field_test gem 0.3.0 for Ruby has unvalidated input. A	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
field_test_gem_for_ruby_on_rails	method call that is expected to return a value from a certain set of inputs can be made to return any input, which can be dangerous depending on how applications use it. If an application treats arbitrary variants as trusted, this can lead to a variety of potential vulnerabilities like SQL injection or cross-site scripting (XSS).	07-09	calculated	20190913146 BID MISC MISC
flightpath -- flightpath	FlightPath 4.x and 5.0-x allows directory traversal and Local File Inclusion through the form_include parameter in an index.php?q=system-handle-form-submit POST request because of an include_once in system_handle_form_submit in modules/system/system.module.	2019-07-10	not yet calculated	CVE-2019-13396 CONFIRM
ge_healthcare -- aestiva_and_aespire	In GE Aestiva and Aespire versions 7100 and 7900, a vulnerability exists where serial devices are connected via an added unsecured terminal server to a TCP/IP network configuration, which could allow an attacker to remotely modify device configuration and silence alarms.	2019-07-10	not yet calculated	CVE-2019-10966 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
glpi_project -- glpi	GLPI GLPI Product 9.3.1 is affected by: Frame and Form tags Injection allowing admins to phish users by putting code in reminder description. The impact is: Admins can phish any user or group of users for credentials / credit cards. The component is: Tools > Reminder > Description .. Set the description to any iframe/form tags and apply. The attack vector is: The attacker puts a login form, the user fills it and clicks on submit .. the request is sent to the attacker domain saving the data. The fixed version is: 9.4.1.	2019-07-12	not yet calculated	CVE-2019-1010310 MISC MISC
glpi_project -- glpi	An issue was discovered in GLPI before 9.4.1. After a successful password reset by a user, it is possible to change that user's password again during the next 24 hours without any information except the associated email address.	2019-07-10	not yet calculated	CVE-2019-13240 MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hewlett_packard_enterprise -- 3par_service_processor	HPE has identified a vulnerability in HPE 3PAR Service Processor (SP) version 4.1 through 4.4. HPE 3PAR Service Processor (SP) version 4.1 through 4.4 has a remote information disclosure vulnerability which can allow for the disruption of the confidentiality, integrity and availability of the Service Processor and any managed 3PAR arrays.	2019-07-09	not yet calculated	CVE-2019-11991 CONFIRM
huawei -- mate_20_and_mate_20_X_honor_magic_2	There is a Factory Reset Protection (FRP) bypass vulnerability on several smartphones. The system does not sufficiently verify the permission, an attacker could do a certain operation on certain step of setup wizard. Successful exploit could allow the attacker bypass the FRP protection. Affected products: Mate 20 X, versions earlier than Ever-AL00B 9.0.0.200(C00E200R2P1); Mate 20, versions earlier than Hima-AL00B/Hima-TL00B 9.0.0.200(C00E200R2P1); Honor Magic 2, versions earlier than Tony-AL00B/Tony-TL00B 9.0.0.182(C00E180R2P2).	2019-07-10	not yet calculated	CVE-2019-5220 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- mate_20_x	There is a path traversal vulnerability on Huawei Share. The software does not properly validate the path, an attacker could crafted a file path when transporting file through Huawei Share, successful exploit could allow the attacker to transport a file to arbitrary path on the phone. Affected products: Mate 20 X versions earlier than Ever-L29B 9.1.0.300(C432E3R1P12), versions earlier than Ever-L29B 9.1.0.300(C636E3R2P1), and versions earlier than Ever-L29B 9.1.0.300(C185E3R3P1).	2019-07-10	not yet calculated	CVE-2019-5221 CONFIRM
hunesion -- i-onenet	In Hunesion i-oneNet version 3.0.7 ~ 3.0.53 and 4.0.4 ~ 4.0.16, the specific upload web module doesn't verify the file extension and type, and an attacker can upload a webshell. After the webshell upload, an attacker can use the webshell to perform remote code exection such as running a system command.	2019-07-10	not yet calculated	CVE-2019-12803 CONFIRM
hunesion -- i-onenet	In Hunesion i-oneNet version 3.0.7 ~ 3.0.53 and 4.0.4 ~ 4.0.16, due to the lack of update file integrity checking in the upgrade process, an attacker can	2019-07-10	not yet calculated	CVE-2019-12804

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	craft malicious file and use it as an update.			CONFIRM
ibm -- content_navigator	IBM Content Navigator 3.0CD is vulnerable to local file inclusion, allowing an attacker to access a configuration file in the ICN server. IBM X-Force ID: 160015.	2019-07-11	not yet calculated	CVE-2019-4263 XF CONFIRM
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 153749.	2019-07-11	not yet calculated	CVE-2018-1968 CONFIRM XF
intel -- processor_diagnostic_tool	Improper access control in the Intel(R) Processor Diagnostic Tool before version 4.1.2.24 may allow an authenticated user to potentially enable escalation of privilege, information disclosure or denial of service via local access.	2019-07-11	not yet calculated	CVE-2019-11133 BID CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				NFIRM
intel -- ssd_dc_s4500_and_s4600_devices	Improper authentication in firmware for Intel(R) SSD DC S4500 Series and Intel(R) SSD DC S4600 Series before SCV10150 may allow an unprivileged user to potentially enable escalation of privilege via physical access.	2019-07-11	not yet calculated	CVE-2018-18095 BID CONFIRM
intuit -- lacerte	Intuit Lacerte 2017 has Incorrect Access Control.	2019-07-09	not yet calculated	CVE-2018-14833 MISC MISC
invoxia -- nvx220_devices	Invoxia NVX220 devices allow TELNET access as admin with a default password.	2019-07-05	not yet calculated	CVE-2018-14528 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ivanti -- endpoint_manager	An issue was discovered in the Core Server in Ivanti Endpoint Manager (EPM) 2017.3 before SU7 and 2018.x before 2018.3 SU3, with remote code execution. In other words, the issue affects 2017.3, 2018.1, and 2018.3 installations that lack the April 2019 update.	2019-07-11	not yet calculated	CVE-2019-10651 CONFIRM
jenkins -- jenkins	Jenkins Port Allocator Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	2019-07-11	not yet calculated	CVE-2019-10350 MLIST MISC
jenkins -- jenkins	A stored cross site scripting vulnerability in Jenkins Dependency Graph Viewer Plugin 0.13 and earlier allowed attackers able to configure jobs in Jenkins to inject arbitrary HTML and JavaScript in the plugin-provided web pages in Jenkins.	2019-07-11	not yet calculated	CVE-2019-10349 MISC MLIST MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	Jenkins Gogs Plugin stored credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	2019-07-11	not yet calculated	CVE-2019-10348 MLIST MISC
jenkins -- jenkins	Jenkins Mashup Portlets Plugin stored credentials unencrypted on the Jenkins master where they can be viewed by users with access to the master file system.	2019-07-11	not yet calculated	CVE-2019-10347 MLIST MISC
jenkins -- jenkins	A reflected cross site scripting vulnerability in Jenkins Embeddable Build Status Plugin 2.0.1 and earlier allowed attackers inject arbitrary HTML and JavaScript into the response of this plugin.	2019-07-11	not yet calculated	CVE-2019-10346 MLIST MISC
jenkins -- jenkins	A missing permission check in Jenkins Docker Plugin 1.1.6 and	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	earlier in various 'fillCredentialsIdItems' methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.	07-11	calculated	2019-10342 MLIST MISC
jenkins -- jenkins	A missing permission check in Jenkins Docker Plugin 1.1.6 and earlier in DockerAPI.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.	2019-07-11	not yet calculated	CVE-2019-10341 MLIST MISC
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Docker Plugin 1.1.6 and earlier in DockerAPI.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.	2019-07-11	not yet calculated	CVE-2019-10340 MLIST MISC
jenkins -- jenkins	Jenkins Caliper CI Plugin stores credentials unencrypted in job	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	07-11	calculated	2019-10351 MLIST MISC
juniper -- junos_os	A vulnerability in the pfe-chassisd Chassis Manager (CMLC) daemon of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) to the EX4300 when specific valid broadcast packets create a broadcast storm condition when received on the me0 interface of the EX4300 Series device. A reboot of the device is required to restore service. Continued receipt of these valid broadcast packets will create a sustained Denial of Service (DoS) against the device. Affected releases are Juniper Networks Junos OS: 16.1 versions above and including 16.1R1 prior to 16.1R7-S5; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R3; 17.3 versions prior to 17.3R3-S2; 17.4 versions prior to 17.4R2; 18.1 versions prior to 18.1R3; 18.2 versions prior to 18.2R2.	2019-07-11	not yet calculated	CVE-2019-0046 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper -- junos_os	On EX4300 Series switches with TCAM optimization enabled, incoming multicast traffic matches an implicit loopback filter rule first, since it has high priority. This rule is meant for reserved multicast addresses 224.0.0.x, but incorrectly matches on 224.x.x.x. Due to this bug, when a firewall filter is applied on the loopback interface, other firewall filters might stop working for multicast traffic. The command 'show firewall filter' can be used to confirm whether the filter is working. This issue only affects the EX4300 switch. No other products or platforms are affected by this vulnerability. This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D51, 14.1X53-D115 on EX4300 Series; 17.1 versions prior to 17.1R3 on EX4300 Series; 17.2 versions prior to 17.2R3-S2 on EX4300 Series; 17.3 versions prior to 17.3R3-S3 on EX4300 Series; 17.4 versions prior to 17.4R2-S5, 17.4R3 on EX4300 Series; 18.1 versions prior to 18.1R3-S1 on EX4300 Series; 18.2 versions prior to 18.2R2 on EX4300 Series; 18.3 versions	2019-07-11	not yet calculated	CVE-2019-0048 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	prior to 18.3R2 on EX4300 Series.			
juniper -- junos_os	On Junos devices with the BGP graceful restart helper mode enabled or the BGP graceful restart mechanism enabled, a certain sequence of BGP session restart on a remote peer that has the graceful restart mechanism enabled may cause the local routing protocol daemon (RPD) process to crash and restart. Repeated crashes of the RPD process can cause prolonged Denial of Service (DoS). Graceful restart helper mode for BGP is enabled by default. No other Juniper Networks products or platforms are affected by this issue. Affected releases are Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S3; 16.2 versions prior to 16.2R2-S9; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R3; 17.2X75 versions prior to 17.2X75-D105; 17.3 versions prior to 17.3R3-S2; 17.4 versions prior to 17.4R1-S7, 17.4R2-S2, 17.4R3; 18.1 versions prior to 18.1R3-S2; 18.2 versions prior to 18.2R2; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30; 18.3 versions prior to 18.3R1-	2019-07-11	not yet calculated	CVE-2019-0049 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	S4, 18.3R2. Junos OS releases prior to 16.1R1 are not affected.			
juniper -- junos_os	The srxpfe process may crash on SRX Series services gateways when the UTM module processes a specific fragmented HTTP packet. The packet is misinterpreted as a regular TCP packet which causes the processor to crash. This issue affects all SRX Series platforms that support URL-Filtering and have web-filtering enabled. Affected releases are Juniper Networks Junos OS: 12.3X48 versions prior to 12.3X48-D85 on SRX Series; 15.1X49 versions prior to 15.1X49-D181, 15.1X49-D190 on SRX Series; 17.3 versions on SRX Series; 17.4 versions prior to 17.4R1-S8, 17.4R2-S5, 17.4R3 on SRX Series; 18.1 versions prior to 18.1R3-S6 on SRX Series; 18.2 versions prior to 18.2R2-S1, 18.2R3 on SRX Series; 18.3 versions prior to 18.3R1-S2, 18.3R2 on SRX Series; 18.4 versions prior to 18.4R1-S1, 18.4R2 on SRX Series.	2019-07-11	not yet calculated	CVE-2019-0052 CONFIRM
juniper -- junos_os	Insufficient validation of environment variables in the telnet client supplied in Junos OS can lead to stack-based	2019-07-11	not yet calcul	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	buffer overflows, which can be exploited to bypass veriexec restrictions on Junos OS. A stack-based overflow is present in the handling of environment variables when connecting via the telnet client to remote telnet servers. This issue only affects the telnet client ? accessible from the CLI or shell ? in Junos OS. Inbound telnet services are not affected by this issue. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S13; 12.3X48 versions prior to 12.3X48-D80; 14.1X53 versions prior to 14.1X53-D130, 14.1X53-D49; 15.1 versions prior to 15.1F6-S12, 15.1R7-S4; 15.1X49 versions prior to 15.1X49-D170; 15.1X53 versions prior to 15.1X53-D237, 15.1X53-D496, 15.1X53-D591, 15.1X53-D69; 16.1 versions prior to 16.1R3-S11, 16.1R7-S4; 16.2 versions prior to 16.2R2-S9; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R1-S8, 17.2R2-S7, 17.2R3-S1; 17.3 versions prior to 17.3R3-S4; 17.4 versions prior to 17.4R1-S6, 17.4R2-S3, 17.4R3; 18.1 versions prior to 18.1R2-S4, 18.1R3-S3; 18.2 versions prior to 18.2R1-S5, 18.2R2-S2, 18.2R3; 18.2X75 versions prior to 18.2X75-D40;		ated	0053 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	18.3 versions prior to 18.3R1-S3, 18.3R2; 18.4 versions prior to 18.4R1-S2, 18.4R2.			
leanote -- leanote	Leanote prior to version 2.6 is affected by: Cross Site Scripting (XSS).	2019-07-11	not yet calculated	CVE-2019-10100003 MISC
libpng -- libpng	libpng before 1.6.32 does not properly check the length of chunks against the user limit.	2019-07-10	not yet calculated	CVE-2017-12652 CONFIRM
linux -- linux_kernel	In the Linux kernel before 5.1.7, a device can be tracked by an attacker using the IP ID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby	2019-07-05	not yet calculated	CVE-2019-10638 BID MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	obtain the hashing key (via enumeration). An attack may be conducted by hosting a crafted web page that uses WebRTC or gQUIC to force UDP traffic to attacker-controlled IP addresses.			MISC MISC MISC MISC MISC MISC
linux -- linux_kernel	The Linux kernel 4.x (starting from 4.1) and 5.x before 5.0.8 allows Information Exposure (partial kernel address disclosure), leading to a KASLR bypass. Specifically, it is possible to extract the KASLR kernel image offset using the IP ID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). This key contains enough bits from a kernel address (of a static variable) so when the key is extracted (via enumeration), the offset of the kernel image is exposed. This	2019-07-05	not yet calculated	CVE-2019-10639 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attack can be carried out remotely, by the attacker forcing the target device to send UDP or ICMP (or certain other) traffic to attacker-controlled IP addresses. Forcing a server to send UDP traffic is trivial if the server is a DNS server. ICMP traffic is trivial if the server answers ICMP Echo requests (ping). For client targets, if the target visits the attacker's web page, then WebRTC or gQUIC can be used to force UDP traffic to attacker-controlled IP addresses. NOTE: this attack against KASLR became viable in 4.1 because IP ID generation was changed to have a dependency on an address associated with a network namespace.			
london_trust_media -- private_internet_access_vpn_client_for_linux	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for Linux could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The openvpn_launcher.64 binary is setuid root. This binary executes /opt/pia/openvpn-64/openvpn, passing the parameters provided from the command line. Care was taken to programmatically	2019-07-11	not yet calculated	CVE-2019-12578 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disable potentially dangerous openvpn parameters; however, the --route-pre-down parameter can be used. This parameter accepts an arbitrary path to a script/program to be executed when OpenVPN exits. The --script-security parameter also needs to be passed to allow for this action to be taken, and --script-security is not currently in the disabled parameter list. A local unprivileged user can pass a malicious script/binary to the --route-pre-down option, which will be executed as root when openvpn is stopped.			
london_trust_media -- private_internet_access_vpn_client_for_linux	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for Linux could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The root_runner.64 binary is setuid root. This binary executes /opt/pia/ruby/64/ruby, which in turn attempts to load several libraries under /tmp/ruby-deploy.old/lib. A local unprivileged user can create a malicious library under this path to execute arbitrary code as the root user.	2019-07-11	not yet calculated	CVE-2019-12575 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
london_trust_media -- private_internet_access_vpn_client_for_linux_and_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for Linux and macOS could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The PIA Linux/macOS binary openvpn_launcher.64 binary is setuid root. This binary accepts several parameters to update the system configuration. These parameters are passed to operating system commands using a "here" document. The parameters are not sanitized, which allow for arbitrary commands to be injected using shell metacharacters. A local unprivileged user can pass special crafted parameters that will be interpolated by the operating system calls.	2019-07-11	not yet calculated	CVE-2019-12579 MISC
london_trust_media -- private_internet_access_vpn_client_for_linux_and_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for Linux and macOS could allow an authenticated, local attacker to overwrite arbitrary files. The openvpn_launcher binary is setuid root. This binary supports the --log option, which accepts a path as an argument. This parameter is not sanitized, which allows a local	2019-07-11	not yet calculated	CVE-2019-12573 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unprivileged user to overwrite arbitrary files owned by any user on the system, including root. This creates a denial of service condition and possible data loss if leveraged by a malicious local user.			
london_trust_media -- private_internet_access_vpn_client_for_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for macOS could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The openvpn_launcher binary is setuid root. This program is called during the connection process and executes several operating system utilities to configure the system. The networksetup utility is called using relative paths. A local unprivileged user can execute arbitrary commands as root by creating a networksetup trojan which will be executed during the connection process. This is possible because the PATH environment variable is not reset prior to executing the OS utility.	2019-07-11	not yet calculated	CVE-2019-12576 MISC
london_trust_media -- private_internet_access_vpn_client_for_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v0.9.8 beta (build 02099) for macOS	2019-07-11	not yet calcul	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could allow an authenticated, local attacker to overwrite arbitrary files. When the client initiates a connection, the XML /tmp/pia-watcher.plist file is created. If the file exists, it will be truncated and the contents completely overwritten. This file is removed on disconnect. An unprivileged user can create a hard or soft link to arbitrary files owned by any user on the system, including root. This creates a denial of service condition and possible data loss if leveraged by a malicious local user.		ated	12571 MISC
london_trust_media -- private_internet_access_vpn_client_for_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for macOS could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The macOS binary openvpn_launcher.64 is setuid root. This binary creates /tmp/pia_upscript.sh when executed. Because the file creation mask (umask) is not reset, the umask value is inherited from the calling process. This value can be manipulated to cause the privileged binary to create files with world writable	2019-07-11	not yet calculated	CVE-2019-12577 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	permissions. A local unprivileged user can modify /tmp/pia_upscript.sh during the connect process to execute arbitrary code as the root user.			
london_trust_media -- private_internet_access_vpn_client_for_windows	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v1.0 for Windows could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The PIA client is vulnerable to a DLL injection vulnerability during the software update process. The updater loads several libraries from a folder that authenticated users have write access to. A low privileged user can leverage this vulnerability to execute arbitrary code as SYSTEM.	2019-07-11	not yet calculated	CVE-2019-12574 MISC
mailenable -- mailenable_enterprise_premium	MailEnable Enterprise Premium 10.23 was vulnerable to multiple directory traversal issues, with which authenticated users could add, remove, or potentially read files in arbitrary folders accessible by the IIS user. This could lead to reading other users' credentials including those of SYSADMIN accounts, reading other users' emails, or adding emails or files to other users' accounts.	2019-07-08	not yet calculated	CVE-2019-12925 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mailenable -- mailenable_enterprise_premium	MailEnable Enterprise Premium 10.23 did not use appropriate access control checks in a number of areas. As a result, it was possible to perform a number of actions, when logged in as a user, that that user should not have had permission to perform. It was also possible to gain access to areas within the application for which the accounts used were supposed to have insufficient access.	2019-07-08	not yet calculated	CVE-2019-12926 CONFIRM MISC
mailenable -- mailenable_enterprise_premium	MailEnable Enterprise Premium 10.23 was vulnerable to stored and reflected cross-site scripting (XSS) attacks. Because the session cookie did not use the HttpOnly flag, it was possible to hijack the session cookie by exploiting this vulnerability.	2019-07-08	not yet calculated	CVE-2019-12927 CONFIRM MISC
mailenable -- mailenable_enterprise_premium	MailEnable Enterprise Premium 10.23 was vulnerable to XML External Entity Injection (XXE) attacks that could be exploited by an unauthenticated user. It was possible for an attacker to use a vulnerability in the configuration of the XML processor to read any file on the host system. Because all	2019-07-08	not yet calculated	CVE-2019-12924 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	credentials were stored in a cleartext file, it was possible to steal all users' credentials (including the highest privileged users).			MISC
mailenable -- mailenable_enterprise_premium	In MailEnable Enterprise Premium 10.23, the potential cross-site request forgery (CSRF) protection mechanism was not implemented correctly and it was possible to bypass it by removing the anti-CSRF token parameter from the request. This could allow an attacker to manipulate a user into unwittingly performing actions within the application (such as sending email, adding contacts, or changing settings) on behalf of the attacker.	2019-07-08	not yet calculated	CVE-2019-12923 CONFIRM MISC
matrixssl -- matrixssl	MatrixSSL before 4.2.1 has an out-of-bounds read during ASN.1 handling.	2019-07-09	not yet calculated	CVE-2019-13470 MISC
minimagick -- minmagick	In lib/mini_magick/image.rb in MiniMagick before 4.9.4, a fetched remote image filename could cause remote command	2019-07-11	not yet calcul	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution because Image.open input is directly passed to Kernel#open, which accepts a '|' character followed by a command.		ated	13574 MISC MISC MISC MISC DEBIAN
mobatech -- mobaxterm	In MobaXterm 11.1, the mobaxterm: URI handler has an argument injection vulnerability that allows remote attackers to execute arbitrary commands when the user visits a specially crafted URL. Based on the available command-line arguments of the software, one can simply inject -exec to execute arbitrary commands. The additional arguments -hideterm and -exitwhendone in the payload make the attack less visible.	2019-07-09	not yet calculated	CVE-2019-13475 MISC
mybb -- mybb	An CSRF issue was discovered in the JN-Jones MyBB-2FA plugin through 2014-11-05 for MyBB. An attacker can forge a request to an installed mybb2fa plugin to control its state via	2019-07-11	not yet calculated	CVE-2019-12363

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	usercp.php?action=mybb2fa&do=deactivate (or usercp.php?action=mybb2fa&do=activate). A deactivate operation lowers the security of the targeted account by disabling two factor authentication.			MISC MISC
netfilter -- iptables	A buffer overflow in iptables-restore in netfilter iptables 1.8.2 allows an attacker to (at least) crash the program or potentially gain code execution via a specially crafted iptables-save file. This is related to add_param_to_argv in xshared.c.	2019-07-12	not yet calculated	CVE-2019-11360 MISC CONFIRM
netiq -- advanced_authentication_framework	A potential Man in the Middle attack (MITM) was found in NetIQ Advanced Authentication Framework versions prior to 6.0.	2019-07-10	not yet calculated	CVE-2019-11650 CONFIRM
npmjs -- serve-here.js	Path traversal vulnerability in version up to v1.1.3 in serve-here.js npm module allows	2019-07-10	not yet calcul	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to list any file in arbitrary folder.		ated	5444 MISC
nuxt -- nuxt.js	@nuxt/devalue before 1.2.3, as used in Nuxt.js before 2.6.2, mishandles object keys, leading to XSS.	2019-07-11	not yet calculated	CVE-2019-13506 MISC MISC MISC MISC MISC MISC
ovirt -- ovirt_metrics	Sensitive passwords used in deployment and configuration of oVirt Metrics, all versions. were found to be insufficiently protected. Passwords could be disclosed in log files (if playbooks are run with -v) or in playbooks stored on Metrics or Bastion hosts.	2019-07-11	not yet calculated	CVE-2019-10194 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
patchwork -- patchwork	A Cross Site Scripting (XSS) vulnerability exists in the template tag used to render message ids in Patchwork v1.1 through v2.1.x. This allows an attacker to insert JavaScript or HTML into the patch detail page via an email sent to a mailing list consumed by Patchwork. This affects the function msgid in templatetags/patch.py. Patchwork versions v2.1.4 and v2.0.4 will contain the fix.	2019-07-10	not yet calculated	CVE-2019-13122 MISC MLIST MISC MISC MISC MISC MISC
php -- php	main/streams/xp_socket.c in PHP 7.x before 2017-03-07 misparses fsockopen calls, such as by interpreting fsockopen('127.0.0.1:80', 443) as if the address/port were 127.0.0.1:80:443, which is later truncated to 127.0.0.1:80. This behavior has a security risk if the explicitly provided port number (i.e., 443 in this example) is hardcoded into an application as a security policy, but the hostname argument (i.e.,	2019-07-10	not yet calculated	CVE-2017-7189 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	127.0.0.1:80 in this example) is obtained from untrusted input.			
prestashop -- prestashop	In PrestaShop before 1.7.6.0 RC2, the id_address_delivery and id_address_invoice parameters are affected by an Insecure Direct Object Reference vulnerability due to a guessable value sent to the web application during checkout. An attacker could leak personal customer information. This is PrestaShop bug #14444.	2019-07-09	not yet calculated	CVE-2019-13461 MISC MISC
project_redcap -- redcap	Multiple stored Cross-site scripting (XSS) issues in the admin panel and survey system in REDCap 8 before 8.10.20 and 9 before 9.1.2 allow an attacker to inject arbitrary malicious HTML or JavaScript code into a user's web browser.	2019-07-11	not yet calculated	CVE-2019-13029 MISC
python -- python	http.cookiejar.DefaultPolicy.domain_return_ok in Lib/http/cookiejar.py in Python before 3.7.3 does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g.,	2019-07-13	not yet calculated	CVE-2018-20852 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	pythonicexample.com to steal cookies for example.com). When a program uses http.cookiejar.DefaultPolicy and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker. This affects 2.x through 2.7.16, 3.x before 3.4.10, 3.5.x before 3.5.7, 3.6.x before 3.6.9, and 3.7.x before 3.7.3.			
quest -- kace	Quest KACE, all versions prior to version 8.0.x, 8.1.x, and 9.0.x, allows unintentional access to the appliance leveraging functions of the troubleshooting tools located in the administrator user interface.	2019-07-08	not yet calculated	CVE-2019-10973 BID MISC
rapid7 -- insight_agent	Rapid7 Insight Agent, version 2.6.3 and prior, suffers from a local privilege escalation due to an uncontrolled DLL search path. Specifically, when Insight Agent 2.6.3 and prior starts, the Python interpreter attempts to load python3.dll at "C:\DLLs\python3.dll," which normally is writable by locally authenticated users. Because of this, a malicious local user could use Insight Agent's startup	2019-07-12	not yet calculated	CVE-2019-5629 MISC FULLDISC MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	conditions to elevate to SYSTEM privileges. This issue was fixed in Rapid7 Insight Agent 2.6.4.			CCONFIRM BUGTRAQ
razor -- surround	The RzSurroundVADStreamingService (RzSurroundVADStreamingService.exe) in Razer Surround 1.1.63.0 runs as the SYSTEM user using an executable located in %PROGRAMDATA%\Razer\Synapse\Devices\Razer Surround\Driver\. The DACL on this folder allows any user to overwrite contents of files in this folder, resulting in Elevation of Privilege.	2019-07-09	not yet calculated	CVE-2019-13142 MISC
realization -- concerto_critical_chain_planner	Realization Concerto Critical Chain Planner (aka CCPM) 5.10.8071 has SQL Injection in at least in the taskupdt/taskdetails.aspx webpage via the projectname parameter.	2019-07-12	not yet calculated	CVE-2019-13027 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
red_hat -- openshift_container_platform	A reflected XSS vulnerability exists in authorization flow of OpenShift Container Platform versions: openshift-online-3, openshift-enterprise-3.4 through 3.7 and openshift-enterprise-3.9 through 3.11. An attacker could use this flaw to steal authorization data by getting them to click on a malicious link.	2019-07-11	not yet calculated	CVE-2019-3889 CONFIRM
rockwell_automation -- panelview_5510	In Rockwell Automation PanelView 5510 (all versions manufactured before March 13, 2019 that have never been updated to v4.003, v5.002, or later), a remote, unauthenticated threat actor with access to an affected PanelView 5510 Graphic Display, upon successful exploit, may boot-up the terminal and gain root-level access to the device?s file system.	2019-07-11	not yet calculated	CVE-2019-10970 BID MISC
sap -- abap_server_and_abap_platform	ABAP Server and ABAP Platform (SAP Basis), versions, 7.31, 7.4, 7.5, do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-07-10	not yet calculated	CVE-2019-0321 BID MISC CO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				NFIRM
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (BI Workspace) (Enterprise), versions 4.1, 4.2, 4.3, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-07-10	not yet calculated	CVE-2019-0326 BID MISC CONFIRM
sap -- commerce_cloud	SAP Commerce Cloud (previously known as SAP Hybris Commerce), (HY_COM, versions 6.3, 6.4, 6.5, 6.6, 6.7, 1808, 1811), allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service.	2019-07-10	not yet calculated	CVE-2019-0322 BID MISC CONFIRM
sap -- diagnostic_agent	The OS Command Plugin in the transaction GPA_ADMIN and the OSCommand Console of SAP Diagnostic Agent (LM-Service), version 7.2, allow an attacker to inject code that can	2019-07-10	not yet calculated	CVE-2019-0330

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	be executed by the application. An attacker could thereby control the behavior of the application.			BID MISC CONFIRM
sap -- erp_hcm	SAP ERP HCM (SAP_HRCES), version 3, does not perform necessary authorization checks for a report that reads payroll data of employees in a certain area. Due to this under certain conditions, the user that once had authorization to payroll data of an employee, which was later revoked, may retain access to the same data.	2019-07-10	not yet calculated	CVE-2019-0325 BID MISC CONFIRM
sap -- netweaver_application_server	Under certain conditions SAP NetWeaver Application Server for Java (Startup Framework), versions 7.21, 7.22, 7.45, 7.49, and 7.53, allows an attacker to access information which would otherwise be restricted.	2019-07-10	not yet calculated	CVE-2019-0318 BID MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- netweaver_for_java_application_server	SAP NetWeaver for Java Application Server - Web Container, (engineapi, versions 7.1, 7.2, 7.3, 7.31, 7.4 and 7.5), (servercode, versions 7.2, 7.3, 7.31, 7.4, 7.5), allows an attacker to upload files (including script files) without proper file format validation.	2019-07-10	not yet calculated	CVE-2019-0327 BID MISC CONFIRM
sap -- netweaver_process_integration	ABAP Tests Modules (SAP Basis, versions 7.0, 7.1, 7.3, 7.31, 7.4, 7.5) of SAP NetWeaver Process Integration enables an attacker the execution of OS commands with privileged rights. An attacker could thereby impact the integrity and availability of the system.	2019-07-10	not yet calculated	CVE-2019-0328 BID MISC CONFIRM
sap -- sap_gateway	The SAP Gateway, versions 7.5, 7.51, 7.52 and 7.53, allows an attacker to inject content which is displayed in the form of an error message. An attacker could thus mislead a user to believe this information is from the legitimate service when it's not.	2019-07-10	not yet calculated	CVE-2019-0319 BID MISC MIS

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
sap -- sapui5_and_openui5	SAPUI5 and OpenUI5, before versions 1.38.39, 1.44.39, 1.52.25, 1.60.6 and 1.63.0, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-07-10	not yet calculated	CVE-2019-0281 BID MISC CONFIRM
schedmd -- slurm	SchedMD Slurm 17.11.x, 18.08.0 through 18.08.7, and 19.05.0 allows SQL Injection.	2019-07-11	not yet calculated	CVE-2019-12838 MISC CONFIRM MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- simatic_pcs_7_and_simatic_wincc_products	A vulnerability has been identified in SIMATIC PCS 7 V8.0 and earlier (All versions), SIMATIC PCS 7 V8.1 (All versions), SIMATIC PCS 7 V8.2 (All versions < V8.2 SP1 with WinCC V7.4 SP1 Upd11), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP2 with WinCC V7.4 SP1 Upd11), SIMATIC WinCC Professional (TIA Portal V13) (All versions), SIMATIC WinCC Professional (TIA Portal V14) (All versions), SIMATIC WinCC Professional (TIA Portal V15) (All versions), SIMATIC WinCC Runtime Professional V13 (All versions), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC V7.2 and earlier (All versions), SIMATIC WinCC V7.3 (All versions), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Upd 11), SIMATIC WinCC V7.5 (All versions < V7.5 Upd 3). The SIMATIC WinCC DataMonitor web application of the affected products allows to upload arbitrary ASPX code. The security vulnerability could be exploited by an authenticated attacker with network access to the WinCC DataMonitor	2019-07-11	not yet calculated	CVE-2019-10935 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	application. No user interaction is required to exploit this vulnerability. The vulnerability impacts confidentiality, integrity, and availability of the affected device. At the stage of publishing this security advisory no public exploitation is known.			
siemens -- siprotec_5_devices	A vulnerability has been identified in SIPROTEC 5 device types 6MD85, 6MD86, 6MD89, 7UM85, 7SA87, 7SD87, 7SL87, 7VK87, 7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86, 7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82, 7UT85, 7UT86, 7UT87 and 7VE85 with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions < V7.90), All other SIPROTEC 5 device types with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions), SIPROTEC 5 relays with CPU variants CP200 and the respective Ethernet communication modules (All versions), DIGSI 5 engineering software (All versions < V7.90). Specially crafted packets sent to port 443/TCP could cause a Denial of Service condition.	2019-07-11	not yet calculated	CVE-2019-10931 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- siprotec_5_devices	A vulnerability has been identified in SIPROTEC 5 device types 6MD85, 6MD86, 6MD89, 7UM85, 7SA87, 7SD87, 7SL87, 7VK87, 7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86, 7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82, 7UT85, 7UT86, 7UT87 and 7VE85 with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions < V7.90), All other SIPROTEC 5 device types with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions), SIPROTEC 5 relays with CPU variants CP200 and the respective Ethernet communication modules (All versions), DIGSI 5 engineering software (All versions < V7.90). A remote attacker could use specially crafted packets sent to port 443/TCP to upload, download or delete files in certain parts of the file system.	2019-07-11	not yet calculated	CVE-2019-10930 MISC
siemens -- spectrum_power_products	A vulnerability has been identified in Spectrum Power 3 (Corporate User Interface) (All versions <= v3.11), Spectrum Power 4 (Corporate User Interface) (Version v4.75), Spectrum Power 5 (Corporate	2019-07-11	not yet calculated	CVE-2019-10933

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	User Interface) (All versions <= v5.50), Spectrum Power 7 (Corporate User Interface) (All versions <= v2.20). The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. User interaction is required for a successful exploitation. The user does not need to be logged into the web interface in order for the exploitation to succeed. At the stage of publishing this security advisory no public exploitation is known.			MISC
siemens -- tia_administrator	A vulnerability has been identified in TIA Administrator (All versions < V1.0 SP1 Upd1). The integrated configuration web application (TIA Administrator) allows to execute certain application commands without proper authentication. The vulnerability could be exploited by an attacker with local access to the affected system. Successful exploitation requires no privileges and no user interaction. An attacker could use the vulnerability to compromise confidentiality and integrity and availability of the affected system. At the time of advisory publication no public	2019-07-11	not yet calculated	CVE-2019-10915 BID MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation of this security vulnerability was known.			
snapview -- mikogo	The Windows versions of Snapview Mikogo, versions before 5.10.2 are affected by insecure implementations which allow local attackers to escalate privileges.	2019-07-12	not yet calculated	CVE-2019-12731 MISC
sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager before 3.17.0 has a weak default of giving any unauthenticated user read permissions on the repository files and images.	2019-07-08	not yet calculated	CVE-2019-9630 MISC
sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager before 3.17.0 establishes a default administrator user with weak defaults (fixed credentials).	2019-07-08	not yet calculated	CVE-2019-9629 MISC
sony -- bravia_smart_tv_devices	Sony BRAVIA Smart TV devices allow remote attackers to cause a denial of service	2019-07-09	not yet calcul	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(device hang) via a crafted web page over HbbTV.		ated	11889 MISC FULLDISC MISC MISC
sony -- bravia_smart_tv_devices	Sony Bravia Smart TV devices allow remote attackers to cause a denial of service (device hang or reboot) via a SYN flood attack over a wired or Wi-Fi LAN.	2019-07-09	not yet calculated	CVE-2019-11890 MISC FULLDISC MISC MISC
spiderlabs -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) 3.0.2. Use of X.Filename instead of X_Filename can bypass some PHP Script Uploads rules,	2019-07-09	not yet calculated	CVE-2019-13464

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	because PHP automatically transforms dots into underscores in certain contexts where dots are invalid.			MISC MISC
squid-cache -- squid	An issue was discovered in Squid 4.0.23 through 4.7. When checking Basic Authentication with HttpHeader::getAuth, Squid uses a global buffer to store the decoded data. Squid does not check that the decoded length isn't greater than the buffer, leading to a heap-based buffer overflow with user controlled data.	2019-07-11	not yet calculated	CVE-2019-12527 CONFIRM CONFIRM CONFIRM
squid-cache -- squid	An issue was discovered in Squid 3.3.9 through 3.5.28 and 4.x through 4.7. When Squid is configured to use Digest authentication, it parses the header Proxy-Authorization. It searches for certain tokens such as domain, uri, and qop. Squid checks if this token's value starts with a quote and ends with one. If so, it performs a memcpy of its length minus 2. Squid never checks whether the value is just a single quote (which would satisfy its requirements), leading	2019-07-11	not yet calculated	CVE-2019-12525 CONFIRM CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to a memcpy of its length minus 1.			
squid-cache -- squid	An issue was discovered in Squid 2.x through 2.7.STABLE9, 3.x through 3.5.28, and 4.x through 4.7. When Squid is configured to use Basic Authentication, the Proxy-Authorization header is parsed via uudecode. uudecode determines how many bytes will be decoded by iterating over the input and checking its table. The length is then used to start decoding the string. There are no checks to ensure that the length it calculates isn't greater than the input buffer. This leads to adjacent memory being decoded as well. An attacker would not be able to retrieve the decoded data unless the Squid maintainer had configured the display of usernames on error pages.	2019-07-11	not yet calculated	CVE-2019-12529 CONFIRM CONFIRM CONFIRM
stopzilla -- stopzilla_antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains an Arbitrary Write vulnerability due to not validating the output buffer address value from IOCtl 0x8000205F.	2019-07-09	not yet calculated	CVE-2018-15738 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC
sunnet -- wmpro	The SUNNET WMPro v5.0 and v5.1 for eLearning system has OS Command Injection via "/teach/course/doajaxfileupload.php". The target server can be exploited without authentication.	2019-07-11	not yet calculated	CVE-2019-11062 CONFIRM CONFIRM CONFIRM
swift -- alliance_web_platform	An issue was discovered in SWIFT Alliance Web Platform 7.1.23. A log injection (and an arbitrary log filename) can be achieved via the PATH_INFO to swp/login/EJBRemoteService/, related to com.swift.ejbgwt.j2ee.client.EjBInvocationException error log information containing null@java:comp/env/ error messages.	2019-07-05	not yet calculated	CVE-2018-16386 MISC
symantec -- messaging_gateway	Symantec Messaging Gateway, prior to 10.7.1, may be	2019-	not yet	CVE-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	07-11	calculated	2019-12751 BID MISC
thoughtspot -- thoughtspot	An authorization bypass vulnerability in pinboard updates in ThoughtSpot 4.4.1 through 5.1.1 (before 5.1.2) allows a low-privilege user with write access to at least one pinboard to corrupt pinboards of another user in the application by spoofing GUIDs in pinboard update requests, effectively deleting them.	2019-07-09	not yet calculated	CVE-2019-12782 MISC CONFIRM CONFIRM
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 contains multiple stack-based buffer overflows when processing user input for the setup wizard, allowing an unauthenticated user to execute arbitrary code. The vulnerability can be exercised on the local intranet or remotely if remote administration is enabled.	2019-07-10	not yet calculated	CVE-2019-13279 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 allows an unauthenticated attacker to execute setup wizard functionality, giving this attacker the ability to change configuration values, potentially leading to a denial of service. The request can be made on the local intranet or remotely if remote administration is enabled.	2019-07-09	not yet calculated	CVE-2019-13277 MISC
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 contains multiple command injections when processing user input for the setup wizard, allowing an unauthenticated user to run arbitrary commands on the device. The vulnerability can be exercised on the local intranet or remotely if remote administration is enabled.	2019-07-10	not yet calculated	CVE-2019-13278 MISC
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 contains a stack-based buffer overflow in the ssi binary. The overflow allows an unauthenticated user to execute arbitrary code by providing a sufficiently long query string when POSTing to any valid cgi,	2019-07-10	not yet calculated	CVE-2019-13276 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	txt, asp, or js file. The vulnerability can be exercised on the local intranet or remotely if remote administration is enabled.			
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 contains a stack-based buffer overflow while returning an error message to the user about failure to resolve a hostname during a ping or traceroute attempt. This allows an authenticated user to execute arbitrary code. The exploit can be exercised on the local intranet or remotely if remote administration is enabled.	2019-07-09	not yet calculated	CVE-2019-13280 MISC
u.s._army -- america's_army_proving_grounds	An issue was discovered in the America's Army Proving Grounds platform for the Unreal Engine. With a false packet sent via UDP, the application server responds with several bytes, giving the possibility of DoS amplification, even being able to be used in DDoS attacks.	2019-07-10	not yet calculated	CVE-2018-10531 MISC MISC
ubiquiti_networks -- edgemax_edgeswitch	Command Injection in EdgeMAX EdgeSwitch prior to 1.8.2 allow an Admin user to execute commands as root.	2019-07-10	not yet calcul	CVE-2019-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
			ated	5446 MISC
ubiquiti_networks -- edgemax_edgeswitch	DoS in EdgeMAX EdgeSwitch prior to 1.8.2 allow an Admin user to Crash the SSH CLI interface by using crafted commands.	2019-07-10	not yet calculated	CVE-2019-5445 MISC
vmware -- esxi	VMware ESXi 6.5 suffers from partial denial of service vulnerability in hostd process. Patch ESXi650-201907201-UG for this issue is available.	2019-07-11	not yet calculated	CVE-2019-5528 BID CONFIRM
wavpack -- wavpack	WavPack 5.1.0 and earlier is affected by: CWE-457: Use of Uninitialized Variable. The impact is: Unexpected control flow, crashes, and segfaults. The component is: ParseWave64HeaderConfig (wave64.c:211). The attack vector is: Maliciously crafted .wav file. The fixed version is:	2019-07-11	not yet calculated	CVE-2019-1010319 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	After commit https://github.com/dbry/WavPack/commit/33a0025d1d63ccd05d9dbaa6923d52b1446a62fe.			MISC
wavpack -- wavpack	WavPack 5.1.0 and earlier is affected by: CWE-457: Use of Uninitialized Variable. The impact is: Unexpected control flow, crashes, and segfaults. The component is: ParseCaffHeaderConfig (caff.c:486). The attack vector is: Maliciously crafted .wav file. The fixed version is: After commit https://github.com/dbry/WavPack/commit/f68a9555b548306c5b1ee45199ccdc4a16a6101b.	2019-07-11	not yet calculated	CVE-2019-1010317 MISC MISC
wavpack -- wavpack	WavPack 5.1 and earlier is affected by: CWE 369: Divide by Zero. The impact is: Divide by zero can lead to sudden crash of a software/service that tries to parse a .wav file. The component is: ParseDsdiffHeaderConfig (dsdiff.c:282). The attack vector is: Maliciously crafted .wav file. The fixed version is: After commit https://github.com/dbry/WavPack/commit/4c0faba32fddbd0745cbfaf1e1aeb3da5d35b9fc.	2019-07-11	not yet calculated	CVE-2019-1010315 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
weseek -- growi	In WESEEK GROWI before 3.5.0, the site-wide basic authentication can be bypassed by adding a URL parameter access_token (this is the parameter used by the API). No valid token is required since it is not validated by the backend. The website can then be browsed as if no basic authentication is required.	2019-07-09	not yet calculated	CVE-2019-13337 MISC
weseek -- growi	In WESEEK GROWI before 3.5.0, a remote attacker can obtain the password hash of the creator of a page by leveraging wiki access to make API calls for page metadata. In other words, the password hash can be retrieved even though it is not a publicly available field.	2019-07-09	not yet calculated	CVE-2019-13338 MISC
wolfvision -- cynap	WolfVision Cynap before 1.30j uses a static, hard-coded cryptographic secret for generating support PINs for the 'forgot password' feature. By knowing this static secret and the corresponding algorithm for calculating support PINs, an attacker can reset the ADMIN password and thus gain remote access.	2019-07-05	not yet calculated	CVE-2019-13352 MISC FULLDISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Rencontre plugin before 3.1.3 for WordPress allows SQL Injection via inc/rencontre_widget.php.	2019-07-08	not yet calculated	CVE-2019-13413 MISC MISC
wordpress -- wordpress	The Rencontre plugin before 3.1.3 for WordPress allows XSS via inc/rencontre_widget.php.	2019-07-08	not yet calculated	CVE-2019-13414 MISC MISC
zeromq -- libzmq	In ZeroMQ libzmq before 4.0.9, 4.1.x before 4.1.7, and 4.2.x before 4.3.2, a remote, unauthenticated client connecting to a libzmq application, running with a socket listening with CURVE encryption/authentication enabled, may cause a stack overflow and overwrite the stack with arbitrary data, due to a buffer overflow in the library. Users running public servers with the above configuration are	2019-07-10	not yet calculated	CVE-2019-13132 MLIST CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	highly encouraged to upgrade as soon as possible, as there are no known mitigations.			MLIST BUGTRAQ UBUNTU DEBIAN
zoho_manageengine -- assetexplorer	An issue was discovered in Zoho ManageEngine AssetExplorer. There is XSS via the SearchN.do search field.	2019-07-11	not yet calculated	CVE-2019-12537 MISC MISC
zoho_manageengine -- servicedesk_plus	An issue was discovered in Zoho ManageEngine ServiceDesk Plus 10.5. There is XSS via the WorkOrder.do search field.	2019-07-11	not yet calculated	CVE-2019-12540 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zoom_video_communications -- zoom_client	In the Zoom Client before 4.4.2 on macOS, remote attackers can cause a denial of service (continual focus grabs) via a sequence of invalid launch?action=join&confno= requests to localhost port 19421.	2019-07-09	not yet calculated	CVE-2019-13449 MISC MISC MISC MISC MISC
zoom_video_communications -- zoom_client	The Zoom Client before 4.4.53932.0709 on macOS allows remote code execution, a different vulnerability than CVE-2019-13450. If the ZoomOpener daemon (aka the hidden web server) is running, but the Zoom Client is not installed or can't be opened, an attacker can remotely execute code with a maliciously crafted launch URL. NOTE: ZoomOpener is removed by the Apple Malware Removal Tool (MRT) if this tool is enabled and has the 2019-07-10 MRTConfigData.	2019-07-12	not yet calculated	CVE-2019-13567 MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zoom_video_communications -- zoom_client_and_ringcentral	In the Zoom Client through 4.4.4 and RingCentral 7.0.136380.0312 on macOS, remote attackers can force a user to join a video call with the video camera active. This occurs because any web site can interact with the Zoom web server on localhost port 19421 or 19424. NOTE: a machine remains vulnerable if the Zoom Client was installed in the past and then uninstalled. Blocking exploitation requires additional steps, such as the ZDisableVideo preference and/or killing the web server, deleting the ~/.zoomus directory, and creating a ~/.zoomus plain file.	2019-07-09	not yet calculated	CVE-2019-13450 BID MISC MISC MISC MISC MISC MISC MISC
zte -- mw_nr8000	ZTE MW NR8000V2.4.4.03 and NR8000V2.4.4.04 are impacted by path traversal vulnerability. Due to path traversal,users can download any files.	2019-07-11	not yet calculated	CVE-2019-3415 MISC

Back to top