SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 06 January 2021

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-36155	An issue was discovered in the Ultimate Member plugin before 2.1.12 for WordPress, aka Unauthenticated Privilege Escalation via User Meta. An attacker could supply an array parameter for sensitive metadata, such as the wp_capabilities user meta that defines a user's role. During the registration process, submitted registration details were passed to the update_profile function, and any metadata was accepted, e.g., wp_capabilities[administrator] for Administrator access.	10.0	More Details
CVE-2020-35949	An issue was discovered in the Quiz and Survey Master plugin before 7.0.1 for WordPress. It made it possible for unauthenticated attackers to upload arbitrary files and achieve remote code execution. If a quiz question could be answered by uploading a file, only the Content-Type header was checked during the upload, and thus the attacker could use text/plain for a .php file.	10.0	More Details
CVE-2020-29492	Dell Wyse ThinOS 8.6 and prior versions contain an insecure default configuration vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to access the writable file and manipulate the configuration of any target specific station.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29491	Dell Wyse ThinOS 8.6 and prior versions contain an insecure default configuration vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to gain access to the sensitive information on the local network, leading to the potential compromise of impacted thin clients.	10.0	More Details
CVE-2020-36157	An issue was discovered in the Ultimate Member plugin before 2.1.12 for WordPress, aka Unauthenticated Privilege Escalation via User Roles. Due to the lack of filtering on the role parameter that could be supplied during the registration process, an attacker could supply the role parameter with a WordPress capability (or any custom Ultimate Member role) and effectively be granted those privileges.	10.0	More Details
CVE-2020-10208	Command Injection in EntoneWebEngine in Amino Communications AK45x series, AK5xx series, AK65x series, Aria6xx series, Aria7/AK7Xx series and Kami7B allows authenticated remote attackers to execute arbitrary commands with root user privileges.	9.9	More Details
CVE-2020-35945	An issue was discovered in the Divi Builder plugin, Divi theme, and Divi Extra theme before 4.5.3 for WordPress. Authenticated attackers, with contributor-level or above capabilities, can upload arbitrary files, including .php files. This occurs because the check for file extensions is on the client side.	9.9	More Details
CVE-2020-35951	An issue was discovered in the Quiz and Survey Master plugin before 7.0.1 for WordPress. It allows users to delete arbitrary files such as wp-config.php file, which could effectively take a site offline and allow an attacker to reinstall with a WordPress instance under their control. This occurred via qsm_remove_file_fd_question, which allowed unauthenticated deletions (even though it was only intended for a person to delete their own quiz-answer files).	9.9	More Details
CVE-2020-17363	USVN (aka User-friendly SVN) before 1.0.9 allows remote code execution via shell metacharacters in the number_start or number_end parameter to LastHundredRequest (aka lasthundredrequestAction) in the Timeline module. NOTE: this may overlap CVE-2020-25069.	9.9	More Details
CVE-2020-35948	An issue was discovered in the XCloner Backup and Restore plugin before 4.2.13 for WordPress. It gave authenticated attackers the ability to modify arbitrary files, including PHP files. Doing so would allow an attacker to achieve remote code execution. The xcloner_restore.php write_file_action could overwrite wp-config.php, for example. Alternatively, an attacker could create an exploit chain to obtain a database dump.	9.9	More Details
CVE-2020-36156	An issue was discovered in the Ultimate Member plugin before 2.1.12 for WordPress, aka Authenticated Privilege Escalation via Profile Update. Any user with wp-admin access to the profile.php page could supply the parameter um-role with a value set to any role (e.g., Administrator) during a profile update, and effectively escalate their privileges.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35219	The ASUS DSL-N17U modem with firmware 1.1.0.2 allows attackers to access the admin interface by changing the admin password without authentication via a POST request to Advanced_System_Content.asp with the uiViewTools_username=admin&uiViewTools_Password= and uiViewTools_PasswordConfirm= substrings.	9.8	More Details
CVE-2020-35895	An issue was discovered in the stack crate before 0.3.1 for Rust. ArrayVec has an out-of-bounds write via element insertion.	9.8	More Details
CVE-2020-35795	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects AC2100 before 1.2.0.72, AC2400 before 1.2.0.72, AC2600 before 1.2.0.72, CBK40 before 2.5.0.10, CBR40 before 2.5.0.10, D7800 before 1.0.1.58, EAX20 before 1.0.0.36, EAX80 before 1.0.1.62, EX7500 before 1.0.0.68, MK62 before 1.0.5.102, MR60 before 1.0.5.102, MS60 before 1.0.5.102, R6120 before 1.0.0.70, R6220 before 1.1.0.100, R6230 before 1.1.0.100, R6260 before 1.1.0.76, R6330 before 1.1.0.76, R6350 before 1.1.0.76, R6400 before 1.0.1.62, R6400v2 before 1.0.4.98, R6700 before 1.0.2.16, R6700v2 before 1.2.0.72, R6700v3 before 1.0.4.98, R6800 before 1.2.0.72, R6850 before 1.1.0.76, R6900P before 1.3.2.124, R6900 before 1.0.2.16, R6900v2 before 1.2.0.72, R7000 before 1.0.11.106, R7000P before 1.3.2.124, R7200 before 1.2.0.72, R7350 before 1.2.0.72, R7400 before 1.2.0.72, R7450 before 1.2.0.72, R7800 before 1.0.2.74, R7850 before 1.0.5.60, R7900 before 1.0.4.26, R7900P before 1.4.1.62, R7960P before 1.4.1.62, R8000 before 1.0.4.58, R8000P before 1.4.1.62, R8900 before 1.0.5.24, R9000 before 1.0.5.24, RAX120 before 1.0.1.136, RAX15 before 1.0.1.64, RAX20 before 1.0.1.64, RAX200 before 1.0.2.102, RAX45 before 1.0.2.64, RAX50 before 1.0.2.64, RAX75 before 1.0.3.102, RAX80 before 1.0.3.102, RBK12 before 2.6.1.44, RBR10 before 2.6.1.44, RBS10 before 2.6.1.44, RBK20 before 2.6.1.38, RBR20 before 2.6.1.36, RBS20 before 2.6.1.38, RBK40 before 2.6.1.38, RBR40 before 2.6.1.36, RBS40 before 2.6.1.38, RBK50 before 2.6.1.40, RBR50 before 2.6.1.40, RBS50 before 2.6.1.40, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK842 before 3.2.16.6, RBR840 before 3.2.16.6, RBS840 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, RBS850 before 3.2.16.6, RS400 before 1.5.0.48, XR300 before 1.0.3.50, XR450 before 2.3.2.66, XR500 before 2.3.2.66, and XR700 before 1.0.1.34.	9.8	More Details
CVE-2020-35873	An issue was discovered in the rusqlite crate before 0.23.0 for Rust. Memory safety can be violated because sessions.rs has a use-after-free.	9.8	More Details
CVE-2020-35876	An issue was discovered in the rio crate through 2020-05-11 for Rust. A struct can be leaked, allowing attackers to obtain sensitive information, cause a use-after-free, or cause a data race.	9.8	More Details
CVE-2020-35877	An issue was discovered in the ozone crate through 2020-07-04 for Rust. Memory safety is violated because of out-of-bounds access.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35878	An issue was discovered in the ozone crate through 2020-07-04 for Rust. Memory safety is violated because of the dropping of uninitialized memory.	9.8	More Details
CVE-2020-35879	An issue was discovered in the rulinalg crate through 2020-02-11 for Rust. There are incorrect lifetime-boundary definitions for RowMut::raw_slice and RowMut::raw_slice_mut.	9.8	More Details
CVE-2020-35880	An issue was discovered in the bigint crate through 2020-05-07 for Rust. It allows a soundness violation.	9.8	More Details
CVE-2020-35881	An issue was discovered in the traitobject crate through 2020-06-01 for Rust. It has false expectations about fat pointers, possibly causing memory corruption in, for example, Rust 2.x.	9.8	More Details
CVE-2020-35885	An issue was discovered in the alpm-rs crate through 2020-08-20 for Rust. StrcCtx performs improper memory deallocation.	9.8	More Details
CVE-2020-35887	An issue was discovered in the arr crate through 2020-08-25 for Rust. There is a buffer overflow in Index and IndexMut.	9.8	More Details
CVE-2020-35888	An issue was discovered in the arr crate through 2020-08-25 for Rust. Uninitialized memory is dropped by Array::new_from_template.	9.8	More Details
CVE-2016-20001	The REST/JSON project 7.x-1.x for Drupal allows node access bypass, aka SA-CONTRIB-2016-033. NOTE: This project is not covered by Drupal's security advisory policy.	9.8	More Details
CVE-2020-36112	CSE Bookstore version 1.0 is vulnerable to time-based blind, boolean-based blind and OR error-based SQL injection in pubid parameter in bookPerPub.php and in cart.php. A successful exploitation of this vulnerability will lead to an attacker dumping the entire database on which the web application is running.	9.8	More Details
CVE-2016-20002	The REST/JSON project 7.x-1.x for Drupal allows comment access bypass, aka SA-CONTRIB-2016-033. NOTE: This project is not covered by Drupal's security advisory policy.	9.8	More Details
CVE-2016-20004	The REST/JSON project 7.x-1.x for Drupal allows field access bypass, aka SA-CONTRIB-2016-033. NOTE: This project is not covered by Drupal's security advisory policy.	9.8	More Details
CVE-2016-20005	The REST/JSON project 7.x-1.x for Drupal allows user registration bypass, aka SA-CONTRIB-2016-033. NOTE: This project is not covered by Drupal's security advisory policy.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3021	ISPConfig before 3.2.2 allows SQL injection.	9.8	More Details
CVE-2020-35869	An issue was discovered in the rusqlite crate before 0.23.0 for Rust. Memory safety can be violated because rusqlite::trace::log mishandles format strings.	9.8	More Details
CVE-2020-26045	FUEL CMS 1.4.11 allows SQL Injection via parameter 'name' in /fuel/permissions/create/. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.	9.8	More Details
CVE-2020-35950	An issue was discovered in the XCloner Backup and Restore plugin before 4.2.153 for WordPress. It allows CSRF (via almost any endpoint).	9.8	More Details
CVE-2021-3018	ipeak Infosystems ibexwebCMS (aka IPeakCMS) 3.5 is vulnerable to an unauthenticated Boolean-based SQL injection via the id parameter on the /cms/print.php page.	9.8	More Details
CVE-2021-3007	Laminas Project laminas-http before 2.14.2, and Zend Framework 3.0.0, has a deserialization vulnerability that can lead to remote code execution if the content is controllable, related to the __destruct method of the Zend\Http\Response\Stream class in Stream.php. NOTE: Zend Framework is no longer supported by the maintainer. NOTE: the laminas-http vendor considers this a "vulnerability in the PHP language itself" but has added certain type checking as a way to prevent exploitation in (unrecommended) use cases where attacker-supplied data can be deserialized	9.8	More Details
CVE-2020-28464	This affects the package djv before 2.1.4. By controlling the schema file, an attacker can run arbitrary JavaScript code on the victim machine.	9.8	More Details
CVE-2020-35870	An issue was discovered in the rusqlite crate before 0.23.0 for Rust. Memory safety can be violated via an Auxdata API use-after-free.	9.8	More Details
CVE-2020-35872	An issue was discovered in the rusqlite crate before 0.23.0 for Rust. Memory safety can be violated via the repr(Rust) type.	9.8	More Details
CVE-2020-35868	An issue was discovered in the rusqlite crate before 0.23.0 for Rust. Memory safety can be violated via UnlockNotification.	9.8	More Details
CVE-2019-7726	modules/banners/funcs/click.php in NukeViet before 4.3.04 has a SQL INSERT statement with raw header data from an HTTP request (e.g., Referer and User-Agent).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35867	An issue was discovered in the rusqlite crate before 0.23.0 for Rust. Memory safety can be violated via create_module.	9.8	More Details
CVE-2016-9026	Exponent CMS before 2.6.0 has improper input validation in fileController.php.	9.8	More Details
CVE-2016-9025	Exponent CMS before 2.6.0 has improper input validation in purchaseOrderController.php.	9.8	More Details
CVE-2016-9023	Exponent CMS before 2.6.0 has improper input validation in cron/find_help.php.	9.8	More Details
CVE-2016-9022	Exponent CMS before 2.6.0 has improper input validation in usersController.php.	9.8	More Details
CVE-2016-9021	Exponent CMS before 2.6.0 has improper input validation in storeController.php.	9.8	More Details
CVE-2020-12658	gssproxy (aka gss-proxy) before 0.8.3 does not unlock cond_mutex before pthread exit in gp_worker_main() in gp_workers.c. NOTE: An upstream comment states "We are already on a shutdown path when running the code in question, so a DoS there doesn't make any sense, and there has been no additional information provided us (as upstream) to indicate why this would be a problem.	9.8	More Details
CVE-2020-11103	JsLink in Webswing before 2.6.12 LTS, and 2.7.x and 20.x before 20.1, allows remote code execution.	9.8	More Details
CVE-2020-35173	The Amaze File Manager application before 3.4.2 for Android does not properly restrict intents for controlling the FTP server (aka services.ftpservice.FTPReceiver.ACTION_START_FTPSERVER and services.ftpservice.FTPReceiver.ACTION_STOP_FTPSERVER).	9.8	More Details
CVE-2019-12768	An issue was discovered on D-Link DAP-1650 devices through v1.03b07 before 1.04B02_J65H Hot Fix. Attackers can bypass authentication via forceful browsing.	9.8	More Details
CVE-2020-29594	Rocket.Chat before 0.74.4, 1.x before 1.3.4, 2.x before 2.4.13, 3.x before 3.7.3, 3.8.x before 3.8.3, and 3.9.x before 3.9.1 mishandles SAML login.	9.8	More Details
CVE-2020-35848	Agentejo Cockpit before 0.11.2 allows NoSQL injection via the Controller/Auth.php newpassword function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35847	Agentejo Cockpit before 0.11.2 allows NoSQL injection via the Controller/Auth.php resetpassword function.	9.8	More Details
CVE-2020-35846	Agentejo Cockpit before 0.11.2 allows NoSQL injection via the Controller/Auth.php check function.	9.8	More Details
CVE-2020-35797	NETGEAR NMS300 devices before 1.6.0.27 are affected by command injection by an unauthenticated attacker.	9.8	More Details
CVE-2019-7725	includes/core/is_user.php in NukeViet before 4.3.04 deserializes the untrusted nvloginhash cookie (i.e., the code relies on PHP's serialization format when JSON can be used to eliminate the risk).	9.8	More Details
CVE-2018-14067	Green Packet WiMax DV-360 2.10.14-g1.0.6.1 devices allow Command Injection, with unauthenticated remote command execution, via a crafted payload to the HTTPS port, because lighttpd listens on all network interfaces (including the external Internet) by default. NOTE: this may overlap CVE-2017-9980.	9.8	More Details
CVE-2020-25848	HGiga MailSherlock contains weak authentication flaw that attackers grant privilege remotely with default password generation mechanism.	9.8	More Details
CVE-2019-25004	An issue was discovered in the flatbuffers crate before 0.6.1 for Rust. Arbitrary bytes can be reinterpreted as a bool, defeating soundness.	9.8	More Details
CVE-2020-35866	An issue was discovered in the rusqlite crate before 0.23.0 for Rust. Memory safety can be violated via VTab / VTabCursor.	9.8	More Details
CVE-2020-35863	An issue was discovered in the hyper crate before 0.12.34 for Rust. HTTP request smuggling can occur. Remote code execution can occur in certain situations with an HTTP server on the loopback interface.	9.8	More Details
CVE-2020-35862	An issue was discovered in the bitvec crate before 0.17.4 for Rust. BitVec to BitBox conversion leads to a use-after-free or double free.	9.8	More Details
CVE-2020-35860	An issue was discovered in the cbox crate through 2020-03-19 for Rust. The CBox API allows dereferencing raw pointers without a requirement for unsafe code.	9.8	More Details
CVE-2020-35858	An issue was discovered in the prost crate before 0.6.1 for Rust. There is stack consumption via a crafted message, causing a denial of service (e.g., x86) or possibly remote code execution (e.g., ARM).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-25010	An issue was discovered in the failure crate through 2019-11-13 for Rust. Type confusion can occur when __private_get_type_id__ is overridden.	9.8	More Details
CVE-2019-25009	An issue was discovered in the http crate before 0.1.20 for Rust. The HeaderMap::Drain API can use a raw pointer, defeating soundness.	9.8	More Details
CVE-2019-25002	An issue was discovered in the sodiumoxide crate before 0.2.5 for Rust. generichash::Digest::eq compares itself to itself and thus has degenerate security properties.	9.8	More Details
CVE-2020-35926	An issue was discovered in the nanorand crate before 0.5.1 for Rust. It caused any random number generator (even ChaCha) to return all zeroes because integer truncation was mishandled.	9.8	More Details
CVE-2020-35902	An issue was discovered in the actix-codec crate before 0.3.0-beta.1 for Rust. There is a use-after-free in Framed.	9.8	More Details
CVE-2020-36052	Directory traversal vulnerability in post-edit.php in MiniCMS V1.10 allows remote attackers to include and execute arbitrary files via the state parameter.	9.8	More Details
CVE-2020-35391	Tenda N300 F3 12.01.01.48 devices allow remote attackers to obtain sensitive information (possibly including an http_passwd line) via a direct request for cgi-bin/DownloadCfg/RouterCfm.cfg, a related issue to CVE-2017-14942. NOTE: the vulnerability report may suggest that either a ? character must be placed after the RouterCfm.cfg filename, or that the HTTP request headers must be unusual, but it is not known why these are relevant to the device's HTTP response behavior.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35800	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects AC2100 before 1.2.0.72, AC2400 before 1.2.0.72, AC2600 before 1.2.0.72, CBK40 before 2.5.0.10, CBR40 before 2.5.0.10, D6000 before 1.0.0.80, D6220 before 1.0.0.60, D6400 before 1.0.0.94, D7000v2 before 1.0.0.62, D7800 before 1.0.3.48, D8500 before 1.0.3.50, DC112A before 1.0.0.48, DGN2200v4 before 1.0.0.114, DM200 before 1.0.0.66, EAX20 before 1.0.0.36, EAX80 before 1.0.1.62, EX2700 before 1.0.1.58, EX3110 before 1.0.1.68, EX3700 before 1.0.0.84, EX3800 before 1.0.0.84, EX3920 before 1.0.0.84, EX6000 before 1.0.0.44, EX6100v2 before 1.0.1.94, EX6110 before 1.0.1.68, EX6120 before 1.0.0.54, EX6130 before 1.0.0.36, EX6150v1 before 1.0.0.46, EX6150v2 before 1.0.1.94, EX6200v1 before 1.0.3.94, EX6250 before 1.0.0.128, EX6400 before 1.0.2.152, EX6400v2 before 1.0.0.128, EX6410 before 1.0.0.128, EX6920 before 1.0.0.54, EX7000 before 1.0.1.90, EX7300 before 1.0.2.152, EX7300v2 before 1.0.0.128, EX7320 before 1.0.0.128, EX7500 before 1.0.0.68, EX7700 before 1.0.0.210, EX8000 before 1.0.1.224, MK62 before 1.0.5.102, MR60 before 1.0.5.102, MS60 before 1.0.5.102, R6120 before 1.0.0.70, R6220 before 1.1.0.100, R6230 before 1.1.0.100, R6250 before 1.0.4.42, R6260 before 1.1.0.76, R6300v2 before 1.0.4.42, R6330 before 1.1.0.76, R6350 before 1.1.0.76, R6400v1 before 1.0.1.62, R6400v2 before 1.0.4.98, R6700v1 before 1.0.2.16, R6700v2 before 1.2.0.72, R6700v3 before 1.0.4.98, R6800 before 1.2.0.72, R6800 before 1.2.0.72, R6850 before 1.1.0.76, R6900 before 1.0.2.16, R6900P before 1.3.2.124, R6900v2 before 1.2.0.72, R7000 before 1.0.11.106, R7000P before 1.3.2.124, R7100LG before 1.0.0.56, R7200 before 1.2.0.72, R7350 before 1.2.0.72, R7400 before 1.2.0.72, R7450 before 1.2.0.72, R7500v2 before 1.0.3.48, R7800 before 1.0.2.74, R7850 before 1.0.5.60, R7900 before 1.0.4.26, R7900P before 1.4.1.62, R7960P before 1.4.1.62, R8000 before 1.0.4.58, R8000P before 1.4.1.62, R8300 before 1.0.2.134, R8500 before 1.0.2.134, R8900 before 1.0.5.24, R9000 before 1.0.5.24, RAX120 before 1.0.1.136, RAX15 before 1.0.1.64, RAX20 before 1.0.1.64, RAX200 before 1.0.5.24, RAX35 before 1.0.3.80, RAX40 before 1.0.3.80, RAX45 before 1.0.2.64, RAX50 before 1.0.2.64, RAX75 before 1.0.3.102, RAX80 before 1.0.3.102, RBK12 before 2.6.1.44, RBR10 before 2.6.1.44, RBS10 before 2.6.1.44, RBK20 before 2.6.1.38, RBR20 before 2.6.1.36, RBS20 before 2.6.1.38, RBK40 before 2.6.1.38, RBR40 before 2.6.1.38, RBS40 before 2.6.1.38, RBK50 before 2.6.1.40, RBR50 before 2.6.1.40, RBS50 before 2.6.1.40, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK842 before 3.2.16.6, RBR840 before 3.2.16.6, RBS840 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, RBS850 before 3.2.16.6, RBS40V before 2.5.1.6, RBS40V-200 before 1.0.0.46, RBS50Y before 2.6.1.40, RBW30 before 2.5.0.4, RS400 before 1.5.0.48, WN2500RPv2 before 1.0.1.56, WN3000RPv3 before 1.0.2.86, WN3500RPv1 before 1.0.0.28, WNDR3400v3 before 1.0.1.32, WNR1000v3 before 1.0.2.78, WNR2000v2 before 1.2.0.12, XR300 before 1.0.3.50, XR450 before 2.3.2.66, XR500 before 2.3.2.66, and XR700 before 1.0.1.34.	9.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35798	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects R6400v2 before 1.0.4.84, R6700v3 before 1.0.4.84, R6900P before 1.3.2.124, R7000 before 1.0.11.100, R7000P before 1.3.2.124, R7800 before 1.0.2.74, R7850 before 1.0.5.60, R7900 before 1.0.4.26, R7960P before 1.4.1.50, R8000 before 1.0.4.52, R7900P before 1.4.1.50, R8000P before 1.4.1.50, RAX15 before 1.0.1.64, RAX20 before 1.0.1.64, RAX200 before 1.0.1.12, RAX45 before 1.0.2.66, RAX50 before 1.0.2.66, RAX75 before 1.0.3.102, RAX80 before 1.0.3.102, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RS400 before 1.5.0.48, and XR300 before 1.0.3.50.	9.3	More Details
CVE-2020-35883	An issue was discovered in the mozwire crate through 2020-08-18 for Rust. A ../ directory-traversal situation allows overwriting local files that have .conf at the end of the filename.	9.1	More Details
CVE-2020-35898	An issue was discovered in the actix-utils crate before 2.0.0 for Rust. The Cell implementation allows obtaining more than one mutable reference to the same data.	9.1	More Details
CVE-2020-35859	An issue was discovered in the lucet-runtime-internals crate before 0.5.1 for Rust. It mishandles sigstack allocation. Guest programs may be able to obtain sensitive information, or guest programs can experience memory corruption.	9.1	More Details
CVE-2020-35892	An issue was discovered in the simple-slab crate before 0.3.3 for Rust. index() allows an out-of-bounds read.	9.1	More Details
CVE-2020-4899	IBM API Connect 5.0.0.0 through 5.0.8.10 could potentially leak sensitive information or allow for data corruption due to plain text transmission of sensitive information across the network. IBM X-Force ID: 190990.	9.1	More Details
CVE-2018-19945	A vulnerability has been reported to affect earlier QNAP devices running QTS 4.3.4 to 4.3.6. Caused by improper limitations of a pathname to a restricted directory, this vulnerability allows for renaming arbitrary files on the target system, if exploited. QNAP have already fixed this vulnerability in the following versions: QTS 4.3.6.0895 build 20190328 (and later) QTS 4.3.4.0899 build 20190322 (and later) This issue does not affect QTS 4.4.x or QTS 4.5.x.	9.1	More Details
CVE-2020-35717	zonote through 0.4.0 allows XSS via a crafted note, with resultant Remote Code Execution (because nodeIntegration in webPreferences is true).	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2020-28735	Plone before 5.2.3 allows SSRF attacks via the tracebacks feature (only available to the Manager role).	8.8	More Details
CVE-2020-19664	DrayTek Vigor2960 1.5.1 allows remote command execution via shell metacharacters in a toLogin2FA action to mainfunction.cgi.	8.8	More Details
CVE-2020-4762	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5_2, 6.0.0.0 through 6.0.3.2, and 6.1.0.0 could allow an authenticated user to create a privileged account due to improper access controls. IBM X-Force ID: 188896.	8.8	More Details
CVE-2019-4728	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5_2, 6.0.0.0 through 6.0.3.2, and 6.1.0.0 could allow a remote attacker to execute arbitrary code on the system, caused by the deserialization of untrusted data. By sending specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code with SYSTEM privileges. IBM X-Force ID: 172452.	8.8	More Details
CVE-2020-36158	mwifiex_cmd_802_11_ad_hoc_start in drivers/net/wireless/marvell/mwifiex/join.c in the Linux kernel through 5.10.4 might allow remote attackers to execute arbitrary code via a long SSID value, aka CID-5c455c5ab332.	8.8	More Details
CVE-2020-4942	IBM Curam Social Program Management 7.0.9 and 7.0.11 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 191942.	8.8	More Details
CVE-2020-4917	IBM Cloud Pak System 2.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 191391.	8.8	More Details
CVE-2021-21495	MK-AUTH through 19.01 K4.9 allows CSRF for password changes via the central/executar_central.php?acao=altsenha_princ URI.	8.8	More Details
CVE-2020-27848	dotCMS before 20.10.1 allows SQL injection, as demonstrated by the /api/v1/containers orderby parameter. The PaginatorOrdered classes that are used to paginate results of a REST endpoints do not sanitize the orderBy parameter and in some cases it is vulnerable to SQL injection attacks. A user must be an authenticated manager in the dotCMS system to exploit this vulnerability.	8.8	More Details
CVE-2020-28734	Plone before 5.2.3 allows XXE attacks via a feature that is explicitly only available to the Manager role.	8.8	More Details
CVE-2020-28736	Plone before 5.2.3 allows XXE attacks via a feature that is protected by an unapplied permission of plone.schemaeditor.ManageSchemata (therefore, only available to the Manager role).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35799	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.78, D6200 before 1.1.00.32, D7000 before 1.0.1.68, D7800 before 1.0.1.56, DM200 before 1.0.0.61, EX2700 before 1.0.1.52, EX6100v2 before 1.0.1.76, EX6150v2 before 1.0.1.76, EX6200v2 before 1.0.1.74, EX6400 before 1.0.2.140, EX7300 before 1.0.2.140, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.38, R6050 before 1.0.1.18, R6080 before 1.0.0.38, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6230 before 1.1.0.80, R6260 before 1.1.0.40, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900v2 before 1.2.0.36, R7500v2 before 1.0.3.40, R7800 before 1.0.2.62, R8900 before 1.0.4.12, R9000 before 1.0.4.12, RBK20 before 2.3.0.28, RBR20 before 2.3.0.28, RBS20 before 2.3.0.28, RBK40 before 2.3.0.28, RBR40 before 2.3.0.28, RBS40 before 2.3.0.28, RBK50 before 2.3.0.32, RBR50 before 2.3.0.32, RBS50 before 2.3.0.32, WN2000RPTv3 before 1.0.1.34, WN3000RPv2 before 1.0.0.78, WN3000RPv2 before 1.0.0.78, WN3000RPv3 before 1.0.2.78, WN3100RPv2 before 1.0.0.66, WNR2000v5 before 1.0.0.70, WNR2020 before 1.1.0.62, XR450 before 2.3.2.32, and XR500 before 2.3.2.32.	8.8	More Details
CVE-2020-35796	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects CBR40 before 2.5.0.10, D6220 before 1.0.0.60, D6400 before 1.0.0.94, D7000v2 before 1.0.0.62, D8500 before 1.0.3.50, DC112A before 1.0.0.48, DGN2200v4 before 1.0.0.114, EAX20 before 1.0.0.36, EAX80 before 1.0.1.62, EX3700 before 1.0.0.84, EX3800 before 1.0.0.84, EX3920 before 1.0.0.84, EX6000 before 1.0.0.44, EX6100 before 1.0.2.28, EX6120 before 1.0.0.54, EX6130 before 1.0.0.36, EX6150 before 1.0.0.46, EX6200 before 1.0.3.94, EX6920 before 1.0.0.54, EX7000 before 1.0.1.90, EX7500 before 1.0.0.68, MK62 before 1.0.5.102, MR60 before 1.0.5.102, MS60 before 1.0.5.102, R6250 before 1.0.4.42, R6300v2 before 1.0.4.42, R6400 before 1.0.1.62, R6400v2 before 1.0.4.98, R6700v3 before 1.0.4.98, R6700 before 1.0.2.16, R6900P before 1.3.2.124, R6900 before 1.0.2.16, R7000 before 1.0.11.106, R7000P before 1.3.2.124, R7100LG before 1.0.0.56, R7850 before 1.0.5.60, R7900 before 1.0.4.26, R7900P before 1.4.1.62, R7960P before 1.4.1.62, R8000 before 1.0.4.58, R8000P before 1.4.1.62, R8300 before 1.0.2.134, R8500 before 1.0.2.134, RAX15 before 1.0.1.64, RAX20 before 1.0.1.64, RAX200 before 1.0.2.102, RAX45 before 1.0.2.32, RAX50 before 1.0.2.32, RAX75 before 1.0.3.102, RAX80 before 1.0.3.102, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK842 before 3.2.16.6, RBR840 before 3.2.16.6, RBS840 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, RBS850 before 3.2.16.6, RBS40V-200 before 1.0.0.46, RBW30 before 2.5.0.4, RS400 before 1.5.0.48, WN2500RPv2 before 1.0.1.56, WN3500RP before 1.0.0.28, WNDR3400v3 before 1.0.1.32, WNR1000v3 before 1.0.2.78, WNR2000v2 before 1.2.0.12, WNR3500Lv2 before 1.2.0.62, and XR300 before 1.0.3.50.	8.8	More Details
CVE-2021-22492	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Broadcom Bluetooth chipsets) software. The Bluetooth UART driver has a buffer overflow. The Samsung ID is SVE-2020-18731 (January 2021).	8.8	More Details
CVE-2020-35944	An issue was discovered in the PageLayer plugin before 1.1.2 for WordPress. The pagelayer_settings_page function is vulnerable to CSRF, which can lead to XSS.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35789	NETGEAR NMS300 devices before 1.6.0.27 are affected by command injection by an authenticated user.	8.8	More Details
CVE-2018-25002	uploader.php in the KCFinder integration project through 2018-06-01 for Drupal mishandles validation, aka SA-CONTRIB-2018-024. NOTE: This project is not covered by Drupal's security advisory policy.	8.8	More Details
CVE-2020-26165	qdPM through 9.1 allows PHP Object Injection via timeReportActions::executeExport in core/apps/qdPM/modules/timeReport/actions/actions.class.php because unserialize is used.	8.8	More Details
CVE-2020-13541	An exploitable local privilege elevation vulnerability exists in the file system permissions of the Mobile-911 Server V2.5 install directory. Depending on the vector chosen, an attacker can overwrite the service executable and execute arbitrary code with System privileges or replace other files within the installation folder that could lead to local privilege escalation.	8.8	More Details
CVE-2018-16795	OpenEMR 5.0.1.3 allows Cross-Site Request Forgery (CSRF) via library/ajax and interface/super, as demonstrated by use of interface/super/manage_site_files.php to upload a .php file.	8.8	More Details
CVE-2020-26296	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs. Vega in an npm package. In Vega before version 5.17.3 there is an XSS vulnerability in Vega expressions. Through a specially crafted Vega expression, an attacker could execute arbitrary javascript on a victim's machine. This is fixed in version 5.17.3	8.7	More Details
CVE-2020-35794	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.4	More Details
CVE-2020-35777	NETGEAR DGN2200v1 devices before v1.0.0.58 are affected by command injection.	8.4	More Details
CVE-2020-35792	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7500v2 before 1.0.3.48, R8900 before 1.0.5.2, R9000 before 1.0.5.2, and R7800 before 1.0.2.68.	8.3	More Details
CVE-2020-35801	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. A TFTP server was found to be active by default. It allows remote authenticated users to update the switch firmware.	8.3	More Details
CVE-2020-35785	NETGEAR DGN2200v1 devices before v1.0.0.60 mishandle HTTPd authentication (aka PSV-2020-0363, PSV-2020-0364, and PSV-2020-0365).	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35781	NETGEAR NMS300 devices before 1.6.0.27 are affected by denial of service.	8.3	More Details
CVE-2020-26297	mdBook is a utility to create modern online books from Markdown files and is written in Rust. In mdBook before version 0.4.5, there is a vulnerability affecting the search feature of mdBook, which could allow an attacker to execute arbitrary JavaScript code on the page. The search feature of mdBook (introduced in version 0.1.4) was affected by a cross site scripting vulnerability that allowed an attacker to execute arbitrary JavaScript code on an user's browser by tricking the user into typing a malicious search query, or tricking the user into clicking a link to the search page with the malicious search query prefilled. mdBook 0.4.5 fixes the vulnerability by properly escaping the search query. Owners of websites built with mdBook have to upgrade to mdBook 0.4.5 or greater and rebuild their website contents with it.	8.2	More Details
CVE-2020-35882	An issue was discovered in the rocket crate before 0.4.5 for Rust. LocalRequest::clone creates more than one mutable references to the same object, possibly causing a data race.	8.1	More Details
CVE-2020-35889	An issue was discovered in the crayon crate through 2020-08-31 for Rust. A TOCTOU issue has a resultant memory safety violation via HandleLike.	8.1	More Details
CVE-2020-35851	HGiga MailSherlock does not validate specific parameters properly. Attackers can use the vulnerability to launch Command inject attacks remotely and execute arbitrary commands of the system.	8.1	More Details
CVE-2020-25843	NHIServiSignAdapter fails to verify the length of digital credential files' path which leads to a heap overflow loophole. Remote attackers can use the leak to execute code without privilege.	8.1	More Details
CVE-2020-25850	The function, view the source code, of HGiga MailSherlock does not validate specific characters. Remote attackers can use this flaw to download arbitrary system files.	8.1	More Details
CVE-2020-10209	Command Injection in the CPE WAN Management Protocol (CWMP) registration in Amino Communications AK45x series, AK5xx series, AK65x series, Aria6xx series, Aria7/AK7Xx series and Kami7B allows man-in-the-middle attackers to execute arbitrary commands with root level privileges.	8.1	More Details
CVE-2020-25844	The digest generation function of NHIServiSignAdapter has not been verified for parameter's length, which leads to a stack overflow loophole. Remote attackers can use the leak to execute code without privilege.	8.1	More Details
CVE-2020-35874	An issue was discovered in the internment crate through 2020-05-28 for Rust. ArcIntern::drop has a race condition and resultant use-after-free.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35871	An issue was discovered in the rusqlite crate before 0.23.0 for Rust. Memory safety can be violated via an Auxdata API data race.	8.1	More Details
CVE-2020-35782	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. The TFTP firmware update mechanism does not properly implement firmware validations, allowing remote attackers to write arbitrary data to internal memory.	8.1	More Details
CVE-2019-20484	An issue was discovered in Viki Vera 4.9.1.26180. A user without access to a project could download or upload project files by opening the Project URL directly in the browser after logging in.	8.1	More Details
CVE-2020-29437	SQL injection in the Buzz module of OrangeHRM through 4.6 allows remote authenticated attackers to execute arbitrary SQL commands via the orangehrmBuzzPlugin/lib/dao/BuzzDao.php loadMorePostsForm[profileUserId] parameter to the buzz/loadMoreProfile endpoint.	8.1	More Details
CVE-2020-35787	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40.	8.0	More Details
CVE-2020-27844	A flaw was found in openjpeg's src/lib/openjp2/t2.c in versions prior to 2.4.0. This flaw allows an attacker to provide crafted input to openjpeg during conversion and encoding, causing an out-of-bounds write. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	7.8	More Details
CVE-2020-13540	An exploitable local privilege elevation vulnerability exists in the file system permissions of the Win-911 Enterprise V4.20.13 install directory via WIN-911 Account Change Utility. Depending on the vector chosen, an attacker can overwrite various executables which could lead to escalation of the privileges when executed.	7.8	More Details
CVE-2020-13539	An exploitable local privilege elevation vulnerability exists in the file system permissions of the Win-911 Enterprise V4.20.13 install directory via “WIN-911 Mobile Runtime” service. Depending on the vector chosen, an attacker can overwrite various executables which could lead to escalation of the privileges when executed.	7.8	More Details
CVE-2020-35931	An issue was discovered in Foxit Reader before 10.1.1 (and before 4.1.1 on macOS) and PhantomPDF before 9.7.5 and 10.x before 10.1.1 (and before 4.1.1 on macOS). An attacker can spoof a certified PDF document via an Evil Annotation Attack because the products fail to consider a null value for a Subtype entry of the Annotation dictionary, in an incremental update.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35963	flb_gzip_compress in flb_gzip.c in Fluent Bit before 1.6.4 has an out-of-bounds write because it does not use the correct calculation of the maximum gzip data-size expansion.	7.8	More Details
CVE-2020-35906	An issue was discovered in the futures-task crate before 0.3.6 for Rust. futures_task::waker may cause a use-after-free in a non-static type situation.	7.8	More Details
CVE-2020-36154	The Application Wrapper in Pearson VUE VTS Installer 2.3.1911 has Full Control permissions for Everyone in the "%SYSTEMDRIVE%\Pearson VUE" directory, which allows local users to obtain administrative privileges via a Trojan horse application.	7.8	More Details
CVE-2021-21234	spring-boot-actuator-logview in a library that adds a simple logfile viewer as spring boot actuator endpoint. It is maven package "eu.hinsch:spring-boot-actuator-logview". In spring-boot-actuator-logview before version 0.2.13 there is a directory traversal vulnerability. The nature of this library is to expose a log file directory via admin (spring boot actuator) HTTP endpoints. Both the filename to view and a base folder (relative to the logging folder root) can be specified via request parameters. While the filename parameter was checked to prevent directory traversal exploits (so that `filename=../somefile` would not work), the base folder parameter was not sufficiently checked, so that `filename=somefile&base=../` could access a file outside the logging base directory). The vulnerability has been patched in release 0.2.13. Any users of 0.2.12 should be able to update without any issues as there are no other changes in that release. There is no workaround to fix the vulnerability other than updating or removing the dependency. However, removing read access of the user the application is run with to any directory not required for running the application can limit the impact. Additionally, access to the logview endpoint can be limited by deploying the application behind a reverse proxy.	7.7	More Details
CVE-2020-26288	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. It is an npm package "parse-server". In Parse Server before version 4.5.0, user passwords involved in LDAP authentication are stored in cleartext. This is fixed in version 4.5.0 by stripping password after authentication to prevent cleartext password storage.	7.7	More Details
CVE-2020-35804	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D7800 before 1.0.1.58, R7800 before 1.0.2.74, R8900 before 1.0.5.18, R9000 before 1.0.5.18, and XR700 before 1.0.1.34.	7.6	More Details
CVE-2020-35788	NETGEAR WAC104 devices before 1.0.4.13 are affected by a buffer overflow by an authenticated user.	7.6	More Details
CVE-2020-35936	Stored Cross-Site Scripting (XSS) vulnerabilities in the Post Grid plugin before 2.0.73 for WordPress allow remote authenticated attackers to import layouts including JavaScript supplied via a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to post_grid_import_xml_layouts.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35909	An issue was discovered in the multihash crate before 0.11.3 for Rust. The from_slice parsing code can panic via unsanitized data from a network server.	7.5	More Details
CVE-2019-25012	The Webform Report project 7.x-1.x-dev for Drupal allows remote attackers to view submissions by visiting the /rss.xml page. NOTE: This project is not covered by Drupal's security advisory policy.	7.5	More Details
CVE-2020-35932	Insecure Deserialization in the Newsletter plugin before 6.8.2 for WordPress allows authenticated remote attackers with minimal privileges (such as subscribers) to use the tpnc_render AJAX action to inject arbitrary PHP objects via the options[inline_edits] parameter. NOTE: exploitability depends on PHP objects that might be present with certain other plugins or themes.	7.5	More Details
CVE-2020-35802	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects CBR40 before 2.5.0.14, RBW30 before 2.6.1.4, RAX75 before 1.0.3.102, RAX80 before 1.0.3.102, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, RBS850 before 3.2.16.6, RBK842 before 3.2.16.6, RBR840 before 3.2.16.6, RBS840 before 3.2.16.6, and RBS40V before 2.6.1.4.	7.5	More Details
CVE-2020-29478	CA Service Catalog 17.2 and 17.3 contain a vulnerability in the default configuration of the Setup Utility that may allow a remote attacker to cause a denial of service condition.	7.5	More Details
CVE-2020-35935	The Advanced Access Manager plugin before 6.6.2 for WordPress allows privilege escalation on profile updates via the aam_user_roles POST parameter if Multiple Role support is enabled. (The mechanism for deciding whether a user was entitled to add a role did not work in various custom-role scenarios.)	7.5	More Details
CVE-2020-25842	The encryption function of NHIServiSignAdapter fail to verify the file path input by users. Remote attacker can access arbitrary files through the flaw without privilege.	7.5	More Details
CVE-2020-35901	An issue was discovered in the actix-http crate before 2.0.0-alpha.1 for Rust. There is a use-after-free in BodyStream.	7.5	More Details
CVE-2020-35937	Stored Cross-Site Scripting (XSS) vulnerabilities in the Team Showcase plugin before 1.22.16 for WordPress allow remote authenticated attackers to import layouts including JavaScript supplied via a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to team_import_xml_layouts.	7.5	More Details
CVE-2020-13654	XWiki Platform before 12.8 mishandles escaping in the property displayer.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35938	PHP Object injection vulnerabilities in the Post Grid plugin before 2.0.73 for WordPress allow remote authenticated attackers to inject arbitrary PHP objects due to insecure unserialization of data supplied in a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to post_grid_import_xml_layouts.	7.5	More Details
CVE-2020-25846	The digest generation function of NHIServiSignAdapter has not been verified for source file path, which leads to the SMB request being redirected to a malicious host, resulting in the leakage of user's credential.	7.5	More Details
CVE-2017-20001	The AES encryption project 7.x and 8.x for Drupal does not sufficiently prevent attackers from decrypting data, aka SA-CONTRIB-2017-027. NOTE: This project is not covered by Drupal's security advisory policy.	7.5	More Details
CVE-2020-36051	Directory traversal vulnerability in page_edit.php in MiniCMS V1.10 allows remote attackers to read arbitrary files via the state parameter.	7.5	More Details
CVE-2020-25845	Multiple functions of NHIServiSignAdapter failed to verify the users' file path, which leads to the SMB request being redirected to a malicious host, resulting in the leakage of user's credential.	7.5	More Details
CVE-2016-20006	The REST/JSON project 7.x-1.x for Drupal allows blockage of user logins, aka SA-CONTRIB-2016-033. NOTE: This project is not covered by Drupal's security advisory policy.	7.5	More Details
CVE-2016-20003	The REST/JSON project 7.x-1.x for Drupal allows user enumeration, aka SA-CONTRIB-2016-033. NOTE: This project is not covered by Drupal's security advisory policy.	7.5	More Details
CVE-2019-25001	An issue was discovered in the serde_cbor crate before 0.10.2 for Rust. The CBOR deserializer can cause stack consumption via nested semantic tags.	7.5	More Details
CVE-2020-35865	An issue was discovered in the os_str_bytes crate before 2.0.0 for Rust. It has false expectations about char::from_u32_unchecked behavior.	7.5	More Details
CVE-2020-35864	An issue was discovered in the flatbuffers crate through 2020-04-11 for Rust. read_scalar (and read_scalar_at) can transmute values without unsafe blocks.	7.5	More Details
CVE-2020-35861	An issue was discovered in the bumpalo crate before 3.2.1 for Rust. The realloc feature allows the reading of unknown memory. Attackers can potentially read cryptographic keys.	7.5	More Details
CVE-2020-35857	An issue was discovered in the trust-dns-server crate before 0.18.1 for Rust. DNS MX and SRV null targets are mishandled, causing stack consumption.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35875	An issue was discovered in the tokio-rustls crate before 0.13.1 for Rust. Excessive memory usage may occur when data arrives quickly.	7.5	More Details
CVE-2019-25007	An issue was discovered in the streebog crate before 0.8.0 for Rust. The Streebog hash function can cause a panic.	7.5	More Details
CVE-2019-25006	An issue was discovered in the streebog crate before 0.8.0 for Rust. The Streebog hash function can produce the wrong answer.	7.5	More Details
CVE-2019-25005	An issue was discovered in the chacha20 crate before 0.2.3 for Rust. A ChaCha20 counter overflow makes it easier for attackers to determine plaintext.	7.5	More Details
CVE-2019-25003	An issue was discovered in the libsecp256k1 crate before 0.3.1 for Rust. Scalar::check_overflow allows a timing side-channel attack; consequently, attackers can obtain sensitive information.	7.5	More Details
CVE-2020-35779	NETGEAR NMS300 devices before 1.6.0.27 are affected by denial of service.	7.5	More Details
CVE-2016-20008	The REST/JSON project 7.x-1.x for Drupal allows session enumeration, aka SA-CONTRIB-2016-033. NOTE: This project is not covered by Drupal's security advisory policy.	7.5	More Details
CVE-2020-35890	An issue was discovered in the ordnung crate through 2020-09-03 for Rust. compact::Vec violates memory safety via out-of-bounds access for large capacity.	7.5	More Details
CVE-2020-35891	An issue was discovered in the ordnung crate through 2020-09-03 for Rust. compact::Vec violates memory safety via a remove() double free.	7.5	More Details
CVE-2020-35893	An issue was discovered in the simple-slab crate before 0.3.3 for Rust. remove() has an off-by-one error, causing memory leakage and a drop of uninitialized memory.	7.5	More Details
CVE-2020-35894	An issue was discovered in the obstack crate before 0.1.4 for Rust. Unaligned references can occur.	7.5	More Details
CVE-2020-35896	An issue was discovered in the ws crate through 2020-09-25 for Rust. The outgoing buffer is not properly limited, leading to a remote memory-consumption attack.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-19941	A vulnerability has been reported to affect QNAP NAS. If exploited, this vulnerability allows an attacker to access sensitive information stored in cleartext inside cookies via certain widely-available tools. QNAP have already fixed this vulnerability in the following versions: QTS 4.5.1.1456 build 20201015 (and later) QuTS hero h4.5.1.1472 build 20201031 (and later) QuTScloud c4.5.2.1379 build 20200730 (and later)	7.5	More Details
CVE-2018-19944	A cleartext transmission of sensitive information vulnerability has been reported to affect certain QTS devices. If exploited, this vulnerability allows a remote attacker to gain access to sensitive information. QNAP have already fixed this vulnerability in the following versions: QTS 4.4.3.1354 build 20200702 (and later)	7.5	More Details
CVE-2019-16747	In MatrixSSL before 4.2.2 Open, the DTLS server can encounter an invalid pointer free (leading to memory corruption and a daemon crash) via a crafted incoming network message, a different vulnerability than CVE-2019-14431.	7.5	More Details
CVE-2016-20007	The REST/JSON project 7.x-1.x for Drupal allows session name guessing, aka SA-CONTRIB-2016-033. NOTE: This project is not covered by Drupal's security advisory policy.	7.5	More Details
CVE-2020-28095	On Tenda AC1200 (Model AC6) 15.03.06.51_multi devices, a large HTTP POST request sent to the change password API will trigger the router to crash and enter an infinite boot loop.	7.5	More Details
CVE-2020-35939	PHP Object injection vulnerabilities in the Team Showcase plugin before 1.22.16 for WordPress allow remote authenticated attackers to inject arbitrary PHP objects due to insecure unserialization of data supplied in a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to team_import_xml_layouts.	7.5	More Details
CVE-2019-16281	Ptarmigan before 0.2.3 lacks API token validation, e.g., an "if (token === apiToken) {return true;} return false;" code block.	7.5	More Details
CVE-2020-29228	EGavilanMedia User Registration and Login System With Admin Panel 1.0 is affected by SQL injection in the User Login Page.	7.5	More Details
CVE-2020-36066	GJSON <1.6.5 allows attackers to cause a denial of service (remote) via crafted JSON.	7.5	More Details
CVE-2020-35488	The fileop module of the NXLog service in NXLog Community Edition 2.10.2150 allows remote attackers to cause a denial of service (daemon crash) via a crafted Syslog payload to the Syslog service. This attack requires a specific configuration. Also, the name of the directory created must use a Syslog field. (For example, on Linux it is not possible to create a .. directory. On Windows, it is not possible to create a CON directory.)	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36067	GJSON <=v1.6.5 allows attackers to cause a denial of service (panic: runtime error: slice bounds out of range) via a crafted GET call.	7.5	More Details
CVE-2020-17519	A change introduced in Apache Flink 1.11.0 (and released in 1.11.1 and 1.11.2 as well) allows attackers to read any file on the local filesystem of the JobManager through the REST interface of the JobManager process. Access is restricted to files accessible by the JobManager process. All users should upgrade to Flink 1.11.3 or 1.12.0 if their Flink instance(s) are exposed. The issue was fixed in commit b561010b0ee741543c3953306037f00d7a9f0801 from apache/flink:master.	7.5	More Details
CVE-2020-17518	Apache Flink 1.5.1 introduced a REST handler that allows you to write an uploaded file to an arbitrary location on the local file system, through a maliciously modified HTTP HEADER. The files can be written to any location accessible by Flink 1.5.1. All users should upgrade to Flink 1.11.3 or 1.12.0 if their Flink instance(s) are exposed. The issue was fixed in commit a5264a6f41524afe8ceadf1d8ddc8c80f323ebc4 from apache/flink:master.	7.5	More Details
CVE-2021-3019	ffay lanproxy 0.1 allows Directory Traversal to read /../conf/config.properties to obtain credentials for a connection to the intranet.	7.5	More Details
CVE-2020-25275	Dovecot before 2.3.13 has Improper Input Validation in lda, lmtp, and imap, leading to an application crash via a crafted email message with certain choices for ten thousand MIME parts.	7.5	More Details
CVE-2020-22550	Veno File Manager 3.5.6 is affected by a directory traversal vulnerability. Using the traversal allows an attacker to download sensitive files from the server.	7.5	More Details
CVE-2020-7771	The package asciitable.js before 1.0.3 are vulnerable to Prototype Pollution via the main function.	7.5	More Details
CVE-2020-29490	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.0.4.0.5.012 contain a Denial of Service vulnerability on NAS Servers with NFS exports. A remote authenticated attacker could potentially exploit this vulnerability and cause Denial of Service (Storage Processor Panic) by sending specially crafted UDP requests.	7.5	More Details
CVE-2020-29500	Dell EMC PowerStore versions prior to 1.0.3.0.5.007 contain a Plain-Text Password Storage Vulnerability in PowerStore T environments. A locally authenticated attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	7.5	More Details
CVE-2020-35962	The sellTokenForLRC function in the vault protocol in the smart contract implementation for Loopring (LRC), an Ethereum token, lacks access control for fee swapping and thus allows price manipulation.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29502	Dell EMC PowerStore versions prior to 1.0.3.0.5.007 contain a Plain-Text Password Storage Vulnerability in PowerStore X & T environments. A locally authenticated attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	7.5	More Details
CVE-2021-3006	The breed function in the smart contract implementation for Farm in Seal Finance (Seal), an Ethereum token, lacks access control and thus allows price manipulation, as exploited in the wild in December 2020 and January 2021.	7.5	More Details
CVE-2020-35965	decode_frame in libavcodec/exr.c in FFmpeg 4.3.1 has an out-of-bounds write because of errors in calculations of when to perform memset zero operations.	7.5	More Details
CVE-2020-28852	In x/text in Go before v0.3.5, a "slice bounds out of range" panic occurs in language.ParseAcceptLanguage while processing a BCP 47 tag. (x/text/language is supposed to be able to parse an HTTP Accept-Language header.)	7.5	More Details
CVE-2020-28851	In x/text in Go 1.15.4, an "index out of range" panic occurs in language.ParseAcceptLanguage while parsing the -u- extension. (x/text/language is supposed to be able to parse an HTTP Accept-Language header.)	7.5	More Details
CVE-2020-35737	In Correspondence Management System (corms) in Newgen eGov 12.0, an attacker can modify other users' profile information by manipulating the unvalidated UserIndex parameter, aka Insecure Direct Object Reference.	7.5	More Details
CVE-2019-15080	An issue was discovered in a smart contract implementation for MORPH Token through 2019-06-05, an Ethereum token. A typo in the constructor of the Owned contract (which is inherited by MORPH Token) allows attackers to acquire contract ownership. A new owner can subsequently obtain MORPH Tokens for free and can perform a DoS attack.	7.5	More Details
CVE-2021-3004	The _deposit function in the smart contract implementation for Stable Yield Credit (yCREDIT), an Ethereum token, has certain incorrect calculations. An attacker can obtain more yCREDIT tokens than they should.	7.5	More Details
CVE-2019-15079	A typo exists in the constructor of a smart contract implementation for EAI through 2019-06-05, an Ethereum token. This vulnerability could be used by an attacker to acquire EAI tokens for free.	7.5	More Details
CVE-2020-35849	An issue was discovered in MantisBT before 2.24.4. An incorrect access check in bug_revision_view_page.php allows an unprivileged attacker to view the Summary field of private issues, as well as bugnotes revisions, gaining access to potentially confidential information via the bugnote_id parameter.	7.5	More Details
CVE-2019-15078	An issue was discovered in a smart contract implementation for AIRDROPX BORN through 2019-05-29, an Ethereum token. The name of the constructor has a typo (wrong case: XBornID versus XBORNID) that allows an attacker to change the owner of the contract and obtain cryptocurrency for free.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35947	An issue was discovered in the PageLayer plugin before 1.1.2 for WordPress. Nearly all of the AJAX action endpoints lacked permission checks, allowing these actions to be executed by anyone authenticated on the site. This happened because nonces were used as a means of authorization, but a nonce was present in a publicly viewable page. The greatest impact was the pagelayer_save_content function that allowed pages to be modified and allowed XSS to occur.	7.4	More Details
CVE-2020-26294	Vela is a Pipeline Automation (CI/CD) framework built on Linux container technology written in Golang. In Vela compiler before version 0.6.1 there is a vulnerability which allows exposure of server configuration. It impacts all users of Vela. An attacker can use Sprig's `env` function to retrieve configuration information, see referenced GHSA for an example. This has been fixed in version 0.6.1. In addition to upgrading, it is recommended to rotate all secrets.	7.4	More Details
CVE-2020-4912	IBM Cloud Pak System 2.3 Self Service Console could allow a privilege escalation by capturing the user request URL when logged in as a privileged user. IBM X-Force ID: 191287.	7.2	More Details
CVE-2020-35780	NETGEAR NMS300 devices before 1.6.0.27 are affected by denial of service.	7.1	More Details
CVE-2020-35740	HGiga MailSherlock does not validate specific URL parameters properly that allows attackers to inject JavaScript syntax for XSS attacks.	7.0	More Details
CVE-2020-35742	HGiga MailSherlock contains a vulnerability of SQL Injection. Attackers can inject and launch SQL commands in a URL parameter.	7.0	More Details
CVE-2020-35743	HGiga MailSherlock contains a SQL injection flaw. Attackers can inject and launch SQL commands in a URL parameter of specific cgi pages.	7.0	More Details
CVE-2020-26181	Dell EMC Isilon OneFS versions 8.1 and later and Dell EMC PowerScale OneFS version 9.0.0 contain a privilege escalation vulnerability on a SmartLock Compliance mode cluster. The compadmin user connecting using ISI PRIV LOGIN SSH or ISI PRIV LOGIN CONSOLE can elevate privileges to the root user if they have ISI PRIV HARDENING privileges.	7.0	More Details
CVE-2020-35741	HGiga MailSherlock does not validate user parameters on multiple login pages. Attackers can use the vulnerability to inject JavaScript syntax for XSS attacks.	7.0	More Details
CVE-2020-35842	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62.	6.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35840	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62.	6.9	More Details
CVE-2020-35841	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, R6700v2 before 1.2.0.62, R6800 before 1.2.0.62, R6900v2 before 1.2.0.62, R7450 before 1.2.0.62, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62.	6.9	More Details
CVE-2020-24386	An issue was discovered in Dovecot before 2.3.13. By using IMAP IDLE, an authenticated attacker can trigger unhibernation via attacker-controlled parameters, leading to access to other users' email messages (and path disclosure).	6.8	More Details
CVE-2020-4928	IBM Cloud Pak System 2.3 could allow a local privileged attacker to upload arbitrary files. By intercepting the request and modifying the file extention, the attacker could execute arbitrary code on the server. IBM X-Force ID: 191705.	6.7	More Details
CVE-2020-7336	Cross Site Request Forgery vulnerability in McAfee Network Security Management (NSM) prior to 10.1.7.35 and NSM 9.x prior to 9.2.9.55 may allow an attacker to change the configuration of the Network Security Manager via a carefully crafted HTTP request.	6.6	More Details
CVE-2020-35850	An SSRF issue was discovered in cockpit-project.org Cockpit 234. NOTE: this is unrelated to the Agentejo Cockpit product. NOTE: the vendor states "I don't think [it] is a big real-life issue.	6.5	More Details
CVE-2020-35884	An issue was discovered in the tiny_http crate through 2020-06-16 for Rust. HTTP Request smuggling can occur via a malformed Transfer-Encoding header.	6.5	More Details
CVE-2020-35933	A Reflected Authenticated Cross-Site Scripting (XSS) vulnerability in the Newsletter plugin before 6.8.2 for WordPress allows remote attackers to trick a victim into submitting a tnpc_render AJAX request containing either JavaScript in an options parameter, or a base64-encoded JSON string containing JavaScript in the encoded_options parameter.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26291	URI.js is a javascript URL mutation library (npm package urijs). In URI.js before version 1.19.4, the hostname can be spoofed by using a backslash (`\`) character followed by an at (`@`) character. If the hostname is used in security decisions, the decision may be incorrect. Depending on library usage and attacker intent, impacts may include allow/block list bypasses, SSRF attacks, open redirects, or other undesired behavior. For example the URL `https://expected-example.com\@observed-example.com` will incorrectly return `observed-example.com` if using an affected version. Patched versions correctly return `expected-example.com`. Patched versions match the behavior of other parsers which implement the WHATWG URL specification, including web browsers and Node's built-in URL class. Version 1.19.4 is patched against all known payload variants. Version 1.19.3 has a partial patch but is still vulnerable to a payload variant.]	6.5	More Details
CVE-2019-20808	In QEMU 4.1.0, an out-of-bounds read flaw was found in the ATI VGA implementation. It occurs in the ati_cursor_define() routine while handling MMIO write operations through the ati_mm_write() callback. A malicious guest could abuse this flaw to crash the QEMU process, resulting in a denial of service.	6.5	More Details
CVE-2020-35783	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, GS116Ev2 before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and JGS524PE before 2.6.0.48. The NSDP protocol version allows unauthenticated remote attackers to obtain all the switch configuration parameters by sending the corresponding read requests.	6.5	More Details
CVE-2018-25001	An issue was discovered in the libpulse-binding crate before 2.5.0 for Rust. proplist::Iterator can cause a use-after-free.	6.5	More Details
CVE-2020-35964	track_header in libavformat/vividas.c in FFmpeg 4.3.1 has an out-of-bounds write because of incorrect extradata packing.	6.5	More Details
CVE-2020-35952	login.php in PHPFusion (aka PHP-Fusion) Andromeda 9.x before 2020-12-30 generates error messages that distinguish between incorrect username and incorrect password (i.e., not a single "Incorrect username or password" message in both cases), which might allow enumeration.	6.5	More Details
CVE-2020-5811	An authenticated path traversal vulnerability exists during package installation in Umbraco CMS <= 8.9.1 or current, which could result in arbitrary files being written outside of the site home and expected paths when installing an Umbraco package.	6.5	More Details
CVE-2020-35791	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7800 before 1.0.2.68, R8900 before 1.0.5.2, and R9000 before 1.0.5.2.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29501	Dell EMC PowerStore versions prior to 1.0.3.0.5.007 contain a Plain-Text Password Storage Vulnerability in PowerStore X & T environments. A locally authenticated attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	6.4	More Details
CVE-2020-35790	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.68, R8900 before 1.0.4.26, and R9000 before 1.0.4.26.	6.4	More Details
CVE-2020-26199	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.0.4.0.5.012 contain a plain-text password storage vulnerability. A user credentials (including the Unisphere admin privilege user) password is stored in a plain text in multiple log files. A local authenticated attacker with access to the log files may use the exposed password to gain access with the privileges of the compromised user.	6.4	More Details
CVE-2020-29489	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.0.4.0.5.012 contains a plain-text password storage vulnerability. A user credentials (including the Unisphere admin privilege user) password is stored in a plain text in a system file. A local authenticated attacker with access to the system files may use the exposed password to gain access with the privileges of the compromised user.	6.4	More Details
CVE-2020-35170	Dell EMC Unisphere for PowerMax versions prior to 9.1.0.9, Dell EMC Unisphere for PowerMax versions prior to 9.0.2.16, and Dell EMC PowerMax OS 5978.221.221 and 5978.479.479 contain a Cross-Site Scripting (XSS) vulnerability. An authenticated malicious user may potentially exploit this vulnerability to inject javascript code and affect other authenticated users' sessions.	6.3	More Details
CVE-2020-35784	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and GS116Ev2 before 2.6.0.48.	6.2	More Details
CVE-2020-26293	HtmlSanitizer is a .NET library for cleaning HTML fragments and documents from constructs that can lead to XSS attacks. In HtmlSanitizer before version 5.0.372, there is a possible XSS bypass if style tag is allowed. If you have explicitly allowed the `<style>` tag, an attacker could craft HTML that includes script after passing through the sanitizer. The default settings disallow the `<style>` tag so there is no risk if you have not explicitly allowed the `<style>` tag. The problem has been fixed in version 5.0.372.	6.1	More Details
CVE-2020-35494	There's a flaw in binutils /opcodes/tic4x-dis.c. An attacker who is able to submit a crafted input file to be processed by binutils could cause usage of uninitialized memory. The highest threat is to application availability with a lower threat to data confidentiality. This flaw affects binutils versions prior to 2.34.	6.1	More Details
CVE-2021-3014	In MikroTik RouterOS through 2021-01-04, the hotspot login page is vulnerable to reflected XSS via the target parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29498	Dell Wyse Management Suite versions prior to 3.1 contain an open redirect vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to redirect application users to arbitrary web URLs by tricking the victim users to click on maliciously crafted links. The vulnerability could be used to conduct phishing attacks that cause users to unknowingly visit malicious sites.	6.1	More Details
CVE-2021-3002	Seo Panel 4.8.0 allows reflected XSS via the seo/seopanel/login.php?sec=forgot email parameter.	6.1	More Details
CVE-2021-3026	Invision Community IPS Community Suite before 4.5.4.2 allows XSS during the quoting of a post or comment.	6.1	More Details
CVE-2020-35830	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35836	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78.	6.1	More Details
CVE-2020-35822	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35815	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35818	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBR20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35819	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35816	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35820	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35814	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35839	Certain NETGEAR devices are affected by Stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78.	6.1	More Details
CVE-2020-35838	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35837	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35821	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35793	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.58, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.5.2, and R9000 before 1.0.5.2.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35813	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, XR700 before 1.0.1.10, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, and RAX120 before 1.0.0.78.	6.1	More Details
CVE-2020-35835	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35817	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35834	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35812	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35833	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35832	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35831	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35811	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35829	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35828	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, RAX120 before 1.0.0.78, and R7500v2 before 1.0.3.46.	6.1	More Details
CVE-2020-35827	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78.	6.1	More Details
CVE-2020-35826	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35825	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35824	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35823	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29230	EGavilanMedia User Registration and Login System With Admin Panel 1.0 is affected by cross-site scripting (XSS) in the Admin Panel - Manage User tab using the Full Name of the user. This vulnerability can result in the attacker injecting the XSS payload in the User Registration section and each time admin visits the manage user section from the admin panel, the XSS triggers and the attacker can steal the cookie according to the crafted payload.	6.1	More Details
CVE-2020-28365	Sentrifugo 3.2 allows Stored Cross-Site Scripting (XSS) vulnerability by inserting a payload within the X-Forwarded-For HTTP header during the login process. When an administrator looks at logs, the payload is executed. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	6.1	More Details
CVE-2020-35805	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35809	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35810	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	6.1	More Details
CVE-2020-35806	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.68, RAX120 before 1.0.0.78, RBK22 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and WN3000RPv2 before 1.0.0.78.	6.0	More Details
CVE-2020-35807	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.68, RAX120 before 1.0.0.78, RBK22 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and WN3000RPv2 before 1.0.0.78.	6.0	More Details
CVE-2019-25013	The iconv feature in the GNU C Library (aka glibc or libc6) through 2.32, when processing invalid multi-byte input sequences in the EUC-KR encoding, may have a buffer over-read.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35496	There's a flaw in bfd_pef_scan_start_address() of bfd/pef.c in binutils which could allow an attacker who is able to submit a crafted file to be processed by objdump to cause a NULL pointer dereference. The greatest threat of this flaw is to application availability. This flaw affects binutils versions prior to 2.34.	5.5	More Details
CVE-2020-35921	An issue was discovered in the miow crate before 0.3.6 for Rust. It has false expectations about the std::net::SocketAddr memory representation.	5.5	More Details
CVE-2020-35923	An issue was discovered in the ordered-float crate before 1.1.1 and 2.x before 2.0.1 for Rust. A NotNan value can contain a NaN.	5.5	More Details
CVE-2020-35904	An issue was discovered in the crossbeam-channel crate before 0.4.4 for Rust. It has incorrect expectations about the relationship between the memory allocation and how many iterator elements there are.	5.5	More Details
CVE-2020-35916	An issue was discovered in the image crate before 0.23.12 for Rust. A Mutable reference has immutable provenance. (In the case of LLVM, the IR may be always correct.)	5.5	More Details
CVE-2020-35917	An issue was discovered in the pyo3 crate before 0.12.4 for Rust. There is a reference-counting error and use-after-free in From<Py<T>>.	5.5	More Details
CVE-2020-35493	A flaw exists in binutils in bfd/pef.c. An attacker who is able to submit a crafted PEF file to be parsed by objdump could cause a heap buffer overflow -> out-of-bounds read that could lead to an impact to application availability. This flaw affects binutils versions prior to 2.34.	5.5	More Details
CVE-2020-35495	There's a flaw in binutils /bfd/pef.c. An attacker who is able to submit a crafted input file to be processed by the objdump program could cause a null pointer dereference. The greatest threat from this flaw is to application availability. This flaw affects binutils versions prior to 2.34.	5.5	More Details
CVE-2020-11835	In /SM8250_Q_Master/android/vendor/oppo_charger/oppo/charger_ic/oppo_da9313.c, failure to check the parameter buf in the function proc_work_mode_write in proc_work_mode_write causes a vulnerability.	5.5	More Details
CVE-2020-35507	There's a flaw in bfd_pef_parse_function_stubs of bfd/pef.c in binutils in versions prior to 2.34 which could allow an attacker who is able to submit a crafted file to be processed by objdump to cause a NULL pointer dereference. The greatest threat of this flaw is to application availability.	5.5	More Details
CVE-2020-27842	There's a flaw in openjpeg's t2 encoder in versions prior to 2.4.0. An attacker who is able to provide crafted input to be processed by openjpeg could cause a null pointer dereference. The highest impact of this flaw is to application availability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11834	In /SM8250_Q_Master/android/vendor/oppo_charger/oppo/oppo_vooc.c, the function proc_fastchg_fw_update_write in proc_fastchg_fw_update_write does not check the parameter len, resulting in a vulnerability.	5.5	More Details
CVE-2020-11833	In /SM8250_Q_Master/android/vendor/oppo_charger/oppo/charger_ic/oppo_mp2650.c, the function mp2650_data_log_write in mp2650_data_log_write does not check the parameter len which causes a vulnerability.	5.5	More Details
CVE-2020-11832	In functions charging_limit_current_write and charging_limit_time_write in /SM8250_Q_Master/android/vendor/oppo_charger/oppo/oppo_charger.c have not checked the parameters, which causes a vulnerability.	5.5	More Details
CVE-2020-35918	An issue was discovered in the branca crate before 0.10.0 for Rust. Decoding tokens (with invalid base62 data) can panic.	5.5	More Details
CVE-2020-35919	An issue was discovered in the net2 crate before 0.2.36 for Rust. It has false expectations about the std::net::SocketAddr memory representation.	5.5	More Details
CVE-2020-35920	An issue was discovered in the socket2 crate before 0.3.16 for Rust. It has false expectations about the std::net::SocketAddr memory representation.	5.5	More Details
CVE-2020-35922	An issue was discovered in the mio crate before 0.7.6 for Rust. It has false expectations about the std::net::SocketAddr memory representation.	5.5	More Details
CVE-2020-27841	There's a flaw in openjpeg in versions prior to 2.4.0 in src/lib/openjp2/pi.c. When an attacker is able to provide crafted input to be processed by the openjpeg encoder, this could cause an out-of-bounds read. The greatest impact from this flaw is to application availability.	5.5	More Details
CVE-2020-35915	An issue was discovered in the futures-intrusive crate before 0.4.0 for Rust. GenericMutexGuard allows cross-thread data races of non-Sync types.	5.5	More Details
CVE-2020-27843	A flaw was found in OpenJPEG in versions prior to 2.4.0. This flaw allows an attacker to provide specially crafted input to the conversion or encoding functionality, causing an out-of-bounds read. The highest threat from this vulnerability is system availability.	5.5	More Details
CVE-2020-35924	An issue was discovered in the try-mutex crate before 0.3.0 for Rust. TryMutex<T> allows cross-thread sending of a non-Send type.	5.5	More Details
CVE-2020-35903	An issue was discovered in the dync crate before 0.5.0 for Rust. VecCopy allows misaligned element access because u8 is not always the type in question.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35900	An issue was discovered in the array-queue crate through 2020-09-26 for Rust. A pop_back() call may lead to a use-after-free.	5.5	More Details
CVE-2020-35899	An issue was discovered in the actix-service crate before 1.0.6 for Rust. The Cell implementation allows obtaining more than one mutable reference to the same data.	5.5	More Details
CVE-2021-3022	An issue was discovered on LG mobile devices with Android OS 10 software. There was no write protection for the MTK protect2 partition. The LG ID is LVE-SMP-200028 (January 2021).	5.5	More Details
CVE-2021-22495	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), Q(10.0), and R(11.0) (Exynos chipsets) software. The Mali GPU driver allows out-of-bounds access and a device reset. The Samsung ID is SVE-2020-19174 (January 2021).	5.5	More Details
CVE-2020-35927	An issue was discovered in the thex crate through 2020-12-08 for Rust. Thex<T> allows cross-thread data races of non-Send types.	5.5	More Details
CVE-2020-35925	An issue was discovered in the magnetic crate before 2.0.1 for Rust. MPMCConsumer and MPMCProducer allow cross-thread sending of a non-Send type.	5.5	More Details
CVE-2021-22494	An issue was discovered in the fingerprint scanner on Samsung Note20 mobile devices with Q(10.0) software. When a screen protector is used, the required image compensation is not present. Consequently, inversion can occur during fingerprint enrollment, and a high False Recognition Rate (FRR) can occur. The Samsung ID is SVE-2020-19216 (January 2021).	5.5	More Details
CVE-2020-28841	MyDrivers64.sys in DriverGenius 9.61.3708.3054 allows attackers to cause a system crash via the ioctl command 0x9c402000 to \\.\MyDrivers0_0_1.	5.5	More Details
CVE-2020-35907	An issue was discovered in the futures-task crate before 0.3.5 for Rust. futures_task::noop_waker_ref allows a NULL pointer dereference.	5.5	More Details
CVE-2020-35910	An issue was discovered in the lock_api crate before 0.4.2 for Rust. A data race can occur because of MappedMutexGuard unsoundness.	5.5	More Details
CVE-2020-27845	There's a flaw in src/lib/openjp2/pi.c of openjpeg in versions prior to 2.4.0. If an attacker is able to provide untrusted input to openjpeg's conversion/encoding functionality, they could cause an out-of-bounds read. The highest impact of this flaw is to application availability.	5.5	More Details
CVE-2020-35908	An issue was discovered in the futures-util crate before 0.3.2 for Rust. FuturesUnordered can lead to data corruption because Sync is mishandled.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35930	Seo Panel 4.8.0 allows stored XSS by an Authenticated User via the url parameter, as demonstrated by the seo/seopanel/websites.php URI.	5.4	More Details
CVE-2020-5810	A stored XSS vulnerability exists in Umbraco CMS <= 8.9.1 or current. An authenticated user authorized to upload media can upload a malicious .svg file which act as a stored XSS payload.	5.4	More Details
CVE-2019-16956	SolarWinds Web Help Desk 12.7.0 allows XSS via the Request Type parameter of a ticket.	5.4	More Details
CVE-2020-5809	A stored XSS vulnerability exists in Umbraco CMS <= 8.9.1 or current. An authenticated user can inject arbitrary JavaScript code into iframes when editing content using the TinyMCE rich-text editor, as TinyMCE is configured to allow iframes by default in Umbraco CMS.	5.4	More Details
CVE-2020-29469	WonderCMS 3.1.3 is affected by cross-site scripting (XSS) in the Menu component. This vulnerability can allow an attacker to inject the XSS payload in the Setting - Menu and each time any user will visits the website directory, the XSS triggers and attacker can steal the cookie according to the crafted payload.	5.4	More Details
CVE-2019-20483	An issue was discovered in Viki Vera 4.9.1.26180. An attacker could set a user's last name to an XSS Payload, and read another user's cookie and use that to login to the application.	5.4	More Details
CVE-2020-35946	An issue was discovered in the All in One SEO Pack plugin before 3.6.2 for WordPress. The SEO Description and Title fields are vulnerable to unsanitized input from a Contributor, leading to stored XSS.	5.4	More Details
CVE-2020-26046	FUEL CMS 1.4.11 has stored XSS in Blocks/Navigation/Site variables. This could lead to cookie stealing and other malicious actions. This vulnerability can be exploited with an authenticated account and also impact other visitors.	5.4	More Details
CVE-2020-29233	WonderCMS 3.1.3 is affected by cross-site scripting (XSS) in the Page description component. This vulnerability can allow an attacker to inject the XSS payload in the Page description and each time any user will visits the website, the XSS triggers and attacker can steal the cookie according to the crafted payload.	5.4	More Details
CVE-2020-29231	EGavilanMedia User Registration and Login System With Admin Panel 1.0 is affected by cross-site scripting (XSS) in the Admin Profile Page. This vulnerability can result in the attacker injecting the XSS payload in Admin Full Name and each time admin visits the Profile page from the admin panel, the XSS triggers.	5.4	More Details
CVE-2020-25797	LimeSurvey 3.21.1 is affected by cross-site scripting (XSS) in the Add Participants Function (First and last name parameters). When the survey participant being edited, e.g. by an administrative user, the JavaScript code will be executed in the browser.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25799	LimeSurvey 3.21.1 is affected by cross-site scripting (XSS) in the Quota component of the Survey page. When the survey quota being viewed, e.g. by an administrative user, the JavaScript code will be executed in the browser.	5.4	More Details
CVE-2019-25011	NetBox through 2.6.2 allows an Authenticated User to conduct an XSS attack against an admin via a GFM-rendered field, as demonstrated by /dcim/sites/add/ comments.	5.4	More Details
CVE-2019-16960	SolarWinds Web Help Desk 12.7.0 allows XSS via a CSV template file with a crafted Location Name field.	5.4	More Details
CVE-2020-29497	Dell Wyse Management Suite versions prior to 3.1 contain a stored cross-site scripting vulnerability. A remote authenticated malicious user with low privileges could exploit this vulnerability to store malicious HTML or JavaScript code under the device tag. When victim users access the submitted data through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application.	5.4	More Details
CVE-2020-36159	Veritas Desktop and Laptop Option (DLO) before 9.5 disclosed operational information on the backup processing status through a URL that did not require authentication.	5.3	More Details
CVE-2020-7202	A potential security vulnerability has been identified in HPE Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4) firmware. The vulnerability could be remotely exploited to disclose the serial number and other information.	5.3	More Details
CVE-2020-28925	Bolt before 3.7.2 does not restrict filter options in a Request in the Twig context, and is therefore inconsistent with the "How to Harden Your PHP for Better Security" guidance.	5.3	More Details
CVE-2019-12953	Dropbear 2011.54 through 2018.76 has an inconsistent failure delay that may lead to revealing valid usernames, a different issue than CVE-2018-15599.	5.3	More Details
CVE-2019-15523	An issue was discovered in LINBIT csync2 through 2.0. It does not correctly check for the return value GNUTLS_E_WARNING_ALERT_RECEIVED of the gnutls_handshake() function. It neglects to call this function again, as required by the design of the API.	5.3	More Details
CVE-2020-28413	In MantisBT 2.24.3, SQL Injection can occur in the parameter "access" of the mc_project_get_users function through the API SOAP.	5.3	More Details
CVE-2020-27534	util/binfmt_misc/check.go in Builder in Docker Engine before 19.03.9 calls os.OpenFile with a potentially unsafe qemu-check temporary pathname, constructed with an empty first argument in an ioutil.TempDir call.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4761	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5_2, 6.0.0.0 through 6.0.3.2, and 6.1.0.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 188895.	5.3	More Details
CVE-2020-5361	Select Dell Client Commercial and Consumer platforms support a BIOS password reset capability that is designed to assist authorized customers who forget their passwords. Dell is aware of unauthorized password generation tools that can generate BIOS recovery passwords. The tools, which are not authorized by Dell, can be used by a physically present attacker to reset BIOS passwords and BIOS-managed Hard Disk Drive (HDD) passwords. An unauthenticated attacker with physical access to the system could potentially exploit this vulnerability to bypass security restrictions for BIOS Setup configuration, HDD access and BIOS pre-boot authentication.	5.1	More Details
CVE-2020-35808	Certain NETGEAR devices are affected by stored XSS. This affects D6100 before 1.0.0.63, DM200 before 1.0.0.61, R7800 before 1.0.2.52, R8900 before 1.0.4.12, R9000 before 1.0.4.12, WN3000RPv2 before 1.0.0.68, and WNR2000v5 before 1.0.0.66.	4.8	More Details
CVE-2020-4909	IBM Cloud Pak System 2.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 191273.	4.8	More Details
CVE-2020-29496	Dell Wyse Management Suite versions prior to 3.1 contain a stored cross-site scripting vulnerability. A remote authenticated malicious user with high privileges could exploit this vulnerability to store malicious HTML or JavaScript code while creating the Enduser. When victim users access the submitted data through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application.	4.8	More Details
CVE-2020-4910	IBM Cloud Pak System 2.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 191274.	4.8	More Details
CVE-2020-35241	FlatPress 1.0.3 is affected by cross-site scripting (XSS) in the Blog Content component. This vulnerability can allow an attacker to inject the XSS payload in Blog content via the admin panel. Each time any user will go to that blog page, the XSS triggers and the attacker can steal the cookie according to the crafted payload.	4.8	More Details
CVE-2020-35240	FluxBB 1.5.11 is affected by cross-site scripting (XSS in the Blog Content component. This vulnerability can allow an attacker to inject the XSS payload in "Blog Content" and each time any user will visit the blog, the XSS triggers and the attacker can able to steal the cookie according to the crafted payload.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21494	MK-AUTH through 19.01 K4.9 allows XSS via the admin/logs_ajax.php tipo parameter. An attacker can leverage this to read the centralmka2 (session token) cookie, which is not set to HTTPOnly.	4.8	More Details
CVE-2020-29477	Invision Community 4.5.4 is affected by cross-site scripting (XSS) in the Field Name field. This vulnerability can allow an attacker to inject the XSS payload in Field Name and each time any user will open that, the XSS triggers and the attacker can able to steal the cookie according to the crafted payload.	4.8	More Details
CVE-2020-4916	IBM Cloud Pak System 2.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 191390.	4.8	More Details
CVE-2020-23249	GigaVUE-OS (GVOS) 5.4 - 5.9 stores a Redis database password in plaintext.	4.7	More Details
CVE-2020-35905	An issue was discovered in the futures-util crate before 0.3.7 for Rust. MutexGuard::map can cause a data race for certain closure situations (in safe code).	4.7	More Details
CVE-2020-35911	An issue was discovered in the lock_api crate before 0.4.2 for Rust. A data race can occur because of MappedRwLockReadGuard unsoundness.	4.7	More Details
CVE-2020-35912	An issue was discovered in the lock_api crate before 0.4.2 for Rust. A data race can occur because of MappedRwLockWriteGuard unsoundness.	4.7	More Details
CVE-2020-35913	An issue was discovered in the lock_api crate before 0.4.2 for Rust. A data race can occur because of RwLockReadGuard unsoundness.	4.7	More Details
CVE-2020-35914	An issue was discovered in the lock_api crate before 0.4.2 for Rust. A data race can occur because of RwLockWriteGuard unsoundness.	4.7	More Details
CVE-2020-35897	An issue was discovered in the atom crate before 0.3.6 for Rust. An unsafe Send implementation allows a cross-thread data race.	4.7	More Details
CVE-2020-35886	An issue was discovered in the arr crate through 2020-08-25 for Rust. An attacker can smuggle non-Sync/Send types across a thread boundary to cause a data race.	4.7	More Details
CVE-2020-35928	An issue was discovered in the concread crate before 0.2.6 for Rust. Attackers can cause an ARCache<K,V> data race by sending types that do not implement Send/Sync.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35786	NETGEAR R7800 devices before 1.0.2.74 are affected by a buffer overflow by an authenticated user.	4.5	More Details
CVE-2020-10206	Use of a Hard-coded Password in VNCserver in Amino Communications AK45x series, AK5xx series, AK65x series, Aria6xx series, Aria7/AK7Xx series and Kami7B allows local attackers to view and interact with the video output of the device.	4.4	More Details
CVE-2020-4913	IBM Cloud Pak System 2.3 could reveal credential information in the HTTP response to a local privileged user. IBM X-Force ID: 191288.	4.4	More Details
CVE-2020-35803	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D6200 before 1.1.00.40, D7000 before 1.0.1.78, R6020 before 1.0.0.46, R6080 before 1.0.0.46, R6120 before 1.0.0.72, R6220 before 1.1.0.100, R6230 before 1.1.0.100, R6260 before 1.1.0.76, R6700v2 before 1.2.0.74, R6800 before 1.2.0.74, R6900v2 before 1.2.0.74, R7450 before 1.2.0.74, AC2100 before 1.2.0.74, AC2400 before 1.2.0.74, and AC2600 before 1.2.0.74.	4.4	More Details
CVE-2020-4918	IBM Cloud Pak System 2.3 could allow l local privileged user to disclose sensitive information due to an insecure direct object reference in sell service console for the Platform System Manager. IBM X-Force ID: 191392.	4.4	More Details
CVE-2020-35934	The Advanced Access Manager plugin before 6.6.2 for WordPress displays the unfiltered user object (including all metadata) upon login via the REST API (aam/v1/authenticate or aam/v2/authenticate). This is a security problem if this object stores information that the user is not supposed to have (e.g., custom metadata added by a different plugin).	4.3	More Details
CVE-2020-35778	Certain NETGEAR devices are affected by CSRF. This affects GS716Tv3 before 6.3.1.36 and GS724Tv4 before 6.3.1.36.	4.3	More Details
CVE-2021-3005	MK-AUTH through 19.01 K4.9 allows remote attackers to obtain sensitive information (e.g., a CPF number) via a modified titulo (aka invoice number) value to the central/recibo.php URI.	4.3	More Details
CVE-2020-11947	iscsi_aio_ioctl_cb in block/iscsi.c in QEMU 4.1.0 has a heap-based buffer over-read that may disclose unrelated information from process memory to an attacker.	3.8	More Details
CVE-2020-4919	IBM Cloud Pak System 2.3 has insufficient logout controls which could allow an authenticated privileged user to impersonate another user on the system. IBM X-Force ID: 191395.	3.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26292	Creeper is an experimental dynamic, interpreted language. The binary release of Creeper Interpreter 1.1.3 contains potential malware. The compromised binary release was available for a few hours between December 26, 2020 at 3:22 PM EST to December 26, 2020 at 11:00 PM EST. If you used the source code, you are **NOT** affected. This only affects the binary releases. The binary of unknown quality has been removed from the release. If you have downloaded the binary, please delete it and run a reputable antivirus scanner to ensure that your computer is clean.	3.1	More Details
CVE-2020-26247	Nokogiri is a Rubygem providing HTML, XML, SAX, and Reader parsers with XPath and CSS selector support. In Nokogiri before version 1.11.0.rc4 there is an XXE vulnerability. XML Schemas parsed by Nokogiri::XML::Schema are trusted by default, allowing external resources to be accessed over the network, potentially enabling XXE or SSRF attacks. This behavior is counter to the security policy followed by Nokogiri maintainers, which is to treat all input as untrusted by default whenever possible. This is fixed in Nokogiri version 1.11.0.rc4.	2.6	More Details
CVE-2020-23250	GigaVUE-OS (GVOS) 5.4 - 5.9 uses a weak algorithm for a hash stored in internal database.	2.3	More Details
CVE-2020-5096	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5071	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5079	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5078	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5077	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5076	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5075	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5074	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5073	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5072	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5070	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5095	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5069	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5068	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5067	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5066	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5065	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5064	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5063	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5062	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5080	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5081	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5082	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5083	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5094	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5093	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5092	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5091	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5090	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5089	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5088	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5087	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5086	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5097	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5098	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5085	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5099	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5060	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5100	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5101	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5084	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5061	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2019-25008	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-25574. Reason: This candidate is a duplicate of CVE-2020-25574. Notes: All CVE users should reference CVE-2020-25574 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-5059	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6892	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6904	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6903	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6902	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6901	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6900	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6899	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6898	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6897	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6896	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6895	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6894	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6893	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6891	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6906	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6890	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6889	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6887	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6886	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6885	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6884	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6883	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6878	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-17537	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-17536	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-17535	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16132	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-24240. Reason: This candidate is a reservation duplicate of CVE-2020-24240. Notes: All CVE users should reference CVE-2020-24240 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-6905	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6907	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5058	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5045	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5057	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5056	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5055	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5054	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5053	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5052	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5051	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5050	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5049	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5048	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5047	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5046	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5044	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-6908	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-5043	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5042	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5041	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5040	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5039	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5038	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5037	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2020-5036	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2020. Notes: none	N/A	More Details
CVE-2021-22493	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-25346. Reason: This candidate is a duplicate of CVE-2021-25346. Notes: All CVE users should reference CVE-2021-25346 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-6911	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6910	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6909	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-6888	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details