SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 14 April 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-2021-23281	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to unauthenticated remote code execution vulnerability. IPM software does not sanitize the date provided via coverterCheckList action in meta_driver_srv.js class. Attackers can send a specially crafted packet to make IPM connect to rouge SNMP server and execute attacker-controlled code.	10.0	More Details
CVE-2021-27602	SAP Commerce, versions - 1808, 1811, 1905, 2005, 2011, Backoffice application allows certain authorized users to create source rules which are translated to drools rule when published to certain modules within the application. An attacker with this authorization can inject malicious code in the source rules and perform remote code execution enabling them to compromise the confidentiality, integrity and availability of the application.	9.9	More Details
CVE-2021-21433	Discord Recon Server is a bot that allows you to do your reconnaissance process from your Discord. Remote code execution in version 0.0.1 would allow remote users to execute commands on the server resulting in serious issues. This flaw is patched in 0.0.2.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10881	Xerox AltaLink B8045/B8055/B8065/B8075/B8090, AltaLink C8030/C8035/C8045/C8055/C8070 with software releases before 103.xxx.030.32000 includes two accounts with weak hard-coded passwords which can be exploited and allow unauthorized access which cannot be disabled.	9.8	More Details
CVE-2021-24223	The N5 Upload Form WordPress plugin through 1.0 suffers from an arbitrary file upload issue in page where a Form from the plugin is embed, as any file can be uploaded. The uploaded filename might be hard to guess as it's generated with md5(uniqid(rand())), however, in the case of misconfigured servers with Directory listing enabled, accessing it is trivial.	9.8	More Details
CVE-2021-0430	In rw_mfc_handle_read_op of rw_mfc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution via a malicious NFC packet with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-178725766	9.8	More Details
CVE-2021-26709	D-Link DSL-320B-D1 devices through EU_1.25 are prone to multiple Stack-Based Buffer Overflows that allow unauthenticated remote attackers to take over a device via the login.xgi user and pass parameters. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.8	More Details
CVE-2020-15390	pyActivity in Pega Platform 8.4.0.237 has a security misconfiguration that leads to an improper access control vulnerability via =GetWebInfo.	9.8	More Details
CVE-2021-21524	Dell SRM versions prior to 4.5.0.1 and Dell SMR versions prior to 4.5.0.1 contain an Untrusted Deserialization Vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability, leading to arbitrary privileged code execution on the vulnerable application. The severity is Critical as this may lead to system compromise by unauthenticated attackers.	9.8	More Details
CVE-2021-30503	The unofficial GLSL Linting extension before 1.4.0 for Visual Studio Code allows remote code execution via a crafted glslangValidatorPath in the workspace configuration.	9.8	More Details
CVE-2021-29003	Genexis PLATINUM 4410 2.1 P4410-V2-1.28 devices allow remote attackers to execute arbitrary code via shell metacharacters to sys_config_valid.xgi, as demonstrated by the sys_config_valid.xgi?exeshell=%60telnetd%20%26%60 URI.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27905	The ReplicationHandler (normally registered at "/replication" under a Solr core) in Apache Solr has a "masterUrl" (also "leaderUrl" alias) parameter that is used to designate another ReplicationHandler on another Solr core to replicate index data into the local core. To prevent a SSRF vulnerability, Solr ought to check these parameters against a similar configuration it uses for the "shards" parameter. Prior to this bug getting fixed, it did not. This problem affects essentially all Solr versions prior to it getting fixed in 8.8.2.	9.8	More Details
CVE-2021-29999	An issue was discovered in Wind River VxWorks through 6.8. There is a possible stack overflow in dhcp server.	9.8	More Details
CVE-2021-22505	Escalation of privileges vulnerability in Micro Focus Operations Agent, affects versions 12.0x, 12.10, 12.11, 12.12, 12.14 and 12.15. The vulnerability could be exploited to escalate privileges and execute code under the account of the Operations Agent.	9.8	More Details
CVE-2021-30175	ZEROF Web Server 1.0 (April 2021) allows SQL Injection via the /HandleEvent endpoint for the login page.	9.8	More Details
CVE-2021-30176	The ZEROF Expert pro/2.0 application for mobile devices allows SQL Injection via the Authorization header to the /v2/devices/add endpoint.	9.8	More Details
CVE-2020-27227	An exploitable unatuhenticated command injection exists in the OpenClinic GA 5.173.3. Specially crafted web requests can cause commands to be executed on the server. An attacker can send a web request with parameters containing specific parameter to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and compromise underlying operating system.	9.8	More Details
CVE-2020-27233	An exploitable SQL injection vulnerability exists in ‘getAssets.jsp’ page of OpenClinic GA 5.173.3 in the supplierUID parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2020-27234	An exploitable SQL injection vulnerability exists in ‘getAssets.jsp’ page of OpenClinic GA 5.173.3 in the serviceUID parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2020-27235	An exploitable SQL injection vulnerability exists in ‘getAssets.jsp’ page of OpenClinic GA 5.173.3 in the description parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27236	An exploitable SQL injection vulnerability exists in 'getAssets.jsp' page of OpenClinic GA 5.173.3 in the compnomenclature parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2021-24222	The WP-Curriculo Vitae Free WordPress plugin through 6.3 suffers from an arbitrary file upload issue in page where the [formCadastro] is embed. The form allows unauthenticated user to register and submit files for their profile picture as well as resume, without any file extension restriction, leading to RCE.	9.8	More Details
CVE-2021-24215	An Improper Access Control vulnerability was discovered in the Controlled Admin Access WordPress plugin before 1.5.2. Uncontrolled access to the website customization functionality and global CMS settings, like /wp-admin/customization.php and /wp-admin/options.php, can lead to a complete compromise of the target resource.	9.8	More Details
CVE-2021-29998	An issue was discovered in Wind River VxWorks before 6.5. There is a possible heap overflow in dhcp client.	9.8	More Details
CVE-2021-1459	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. Cisco has not released software updates that address this vulnerability.	9.8	More Details
CVE-2021-30177	There is a SQL Injection vulnerability in PHP-Nuke 8.3.3 in the User Registration section, leading to remote code execution. This occurs because the U.S. state is not validated to be two letters, and the OrderBy field is not validated to be one of LASTNAME, CITY, or STATE.	9.8	More Details
CVE-2021-28481	Microsoft Exchange Server Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-28480	Microsoft Exchange Server Remote Code Execution Vulnerability	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30454	An issue was discovered in the outer_cgi crate before 0.2.1 for Rust. A user-provided Read instance receives an uninitialized memory buffer from KeyValueReader.	9.8	More Details
CVE-2021-30455	An issue was discovered in the id-map crate through 2021-02-26 for Rust. A double free can occur in IdMap::clone_from upon a .clone panic.	9.8	More Details
CVE-2021-30456	An issue was discovered in the id-map crate through 2021-02-26 for Rust. A double free can occur in get_or_insert upon a panic of a user-provided f function.	9.8	More Details
CVE-2021-30457	An issue was discovered in the id-map crate through 2021-02-26 for Rust. A double free can occur in remove_set upon a panic in a Drop impl.	9.8	More Details
CVE-2021-28925	SQL injection vulnerability in Nagios Network Analyzer before 2.4.3 via the o[col] parameter to api/checks/read/.	9.8	More Details
CVE-2020-28872	An authorization bypass vulnerability in Monitorr v1.7.6m in Monitorr/assets/config/_installation/_register.php allows an unauthorized person to create valid credentials.	9.8	More Details
CVE-2020-23426	zzcms 201910 contains an access control vulnerability through escalation of privileges in /user/adv.php, which allows an attacker to modify data for further attacks such as CSRF.	9.8	More Details
CVE-2021-22507	Authentication bypass vulnerability in Micro Focus Operations Bridge Manager affects versions 2019.05, 2019.11, 2020.05 and 2020.10. The vulnerability could allow remote attackers to bypass user authentication and get unauthorized access.	9.8	More Details
CVE-2020-23763	SQL injection in admin.php in Online Book Store 1.0 allows remote attackers to execute arbitrary SQL commands and bypass authentication.	9.8	More Details
CVE-2021-20021	A vulnerability in the SonicWall Email Security version 10.0.9.x allows an attacker to create an administrative account by sending a crafted HTTP request to the remote host.	9.8	More Details
CVE-2021-20020	A command execution vulnerability in SonicWall GMS 9.3 allows a remote unauthenticated attacker to locally escalate privilege to root.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36318	In the standard library in Rust before 1.49.0, VecDeque::make_contiguous has a bug that pops the same element more than once under certain condition. This bug could result in a use-after-free or double free.	9.8	More Details
CVE-2021-28879	In the standard library in Rust before 1.52.0, the Zip implementation can report an incorrect size due to an integer overflow. This bug can lead to a buffer overflow when a consumed Zip iterator is used again.	9.8	More Details
CVE-2021-21730	A ZTE product is impacted by improper access control vulnerability. The attacker could exploit this vulnerability to access CLI by brute force attacks.This affects: ZXHN H168N V3.5.0_TY.T6	9.8	More Details
CVE-2021-24229	The Jetpack Scan team identified a Reflected Cross-Site Scripting via the patreon_save_attachment_patreon_level AJAX action of the Patreon WordPress plugin before 1.7.2. This AJAX hook is used to update the pledge level required by Patreon subscribers to access a given attachment. This action is accessible for user accounts with the 'manage_options' privilege (i.e.., only administrators). Unfortunately, one of the parameters used in this AJAX endpoint is not sanitized before being printed back to the user, so the risk it represents is the same as the previous XSS vulnerability.	9.6	More Details
CVE-2021-24228	The Jetpack Scan team identified a Reflected Cross-Site Scripting in the Login Form of the Patreon WordPress plugin before 1.7.2. The WordPress login form (wp-login.php) is hooked by the plugin and offers to allow users to authenticate on the site using their Patreon account. Unfortunately, some of the error logging logic behind the scene allowed user-controlled input to be reflected on the login page, unsanitized.	9.6	More Details
CVE-2021-21425	Grav Admin Plugin is an HTML user interface that provides a way to configure Grav and create and modify pages. In versions 1.10.7 and earlier, an unauthenticated user can execute some methods of administrator controller without needing any credentials. Particular method execution will result in arbitrary YAML file creation or content change of existing YAML files on the system. Successfully exploitation of that vulnerability results in configuration changes, such as general site information change, custom scheduler job definition, etc. Due to the nature of the vulnerability, an adversary can change some part of the webpage, or hijack an administrator account, or execute operating system command under the context of the web-server user. This vulnerability is fixed in version 1.10.8. Blocking access to the `/admin` path from untrusted sources can be applied as a workaround.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11210	Possible memory corruption in RPM region due to improper XPU configuration in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	9.3	More Details
CVE-2021-29943	When using ConfigurableInternodeAuthHadoopPlugin for authentication, Apache Solr versions prior to 8.8.2 would forward/proxy distributed requests using server credentials instead of original client credentials. This would result in incorrect authorization resolution on the receiving hosts.	9.1	More Details
CVE-2021-24220	Thrive “Legacy” Rise by Thrive Themes WordPress theme before 2.0.0, Luxe by Thrive Themes WordPress theme before 2.0.0, Minus by Thrive Themes WordPress theme before 2.0.0, Ignition by Thrive Themes WordPress theme before 2.0.0, FocusBlog by Thrive Themes WordPress theme before 2.0.0, Squared by Thrive Themes WordPress theme before 2.0.0, Voice WordPress theme before 2.0.0, Performag by Thrive Themes WordPress theme before 2.0.0, Pressive by Thrive Themes WordPress theme before 2.0.0, Storied by Thrive Themes WordPress theme before 2.0.0 register a REST API endpoint to compress images using the Kraken image optimization engine. By supplying a crafted request in combination with data inserted using the Option Update vulnerability, it was possible to use this endpoint to retrieve malicious code from a remote URL and overwrite an existing file on the site with it or create a new file.This includes executable PHP files that contain malicious code.	9.1	More Details
CVE-2021-21399	Ampache is a web based audio/video streaming application and file manager. Versions prior to 4.4.1 allow unauthenticated access to Ampache using the subsonic API. To successfully make the attack you must use a username that is not part of the site to bypass the auth checks. For more details and workaround guidance see the referenced GitHub security advisory.	9.1	More Details
CVE-2021-30246	In the jsrsasign package through 10.1.13 for Node.js, some invalid RSA PKCS#1 v1.5 signatures are mistakenly recognized to be valid. NOTE: there is no known practical attack.	9.1	More Details
CVE-2021-25360	An improper input validation vulnerability in libswmfextractor library prior to SMR APR-2021 Release 1 allows attackers to execute arbitrary code on mediaextractor process.	9.0	More Details
CVE-2021-28483	Microsoft Exchange Server Remote Code Execution Vulnerability	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-28339	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28344	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28335	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28336	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28337	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28338	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-29054	Certain Papoo products are affected by: Cross Site Request Forgery (CSRF) in the admin interface. This affects Papoo CMS Light through 21.02 and Papoo CMS Pro through 6.0.1. The impact is: gain privileges (remote).	8.8	More Details
CVE-2021-28340	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-25328	Skyworth Digital Technology RN510 V.3.1.0.4 RN510 V.3.1.0.4 contains a buffer overflow vulnerability in /cgi-bin/app-staticIP.asp. An authenticated attacker can send a specially crafted request to endpoint which can lead to a denial of service (DoS) or possible code execution on the device.	8.8	More Details
CVE-2021-28341	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-21884	Unibox SMB 2.4 and UniBox Enterprise Series 2.4 and UniBox Campus Series 2.4 contain a cross-site request forgery (CSRF) vulnerability in /tools/network-trace, /list_users, /list_byod?usertype=raduser, /dhcp_leases, /go?rid=202 in which a specially crafted HTTP request may reconfigure the device.	8.8	More Details
CVE-2020-21883	Unibox U-50 2.4 and UniBox Enterprise Series 2.4 and UniBox Campus Series 2.4 contain a OS command injection vulnerability in /tools/ping, which can leads to complete device takeover.	8.8	More Details
CVE-2021-28342	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28343	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28345	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28434	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28346	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28352	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-27522	Learnsite 1.2.5.0 contains a remote privilege escalation vulnerability in /Manager/index.aspx through the JudgIsAdmin() function. By modifying the initial letter of the key of a user cookie, the key of the administrator cookie can be obtained.	8.8	More Details
CVE-2021-30123	FFmpeg <=4.3 contains a buffer overflow vulnerability in libavcodec through a crafted file that may lead to remote code execution.	8.8	More Details
CVE-2021-28353	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28354	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-26758	Privilege Escalation in LiteSpeed Technologies OpenLiteSpeed web server version 1.7.8 allows attackers to gain root terminal access and execute commands on the host system.	8.8	More Details
CVE-2021-29641	Directus 8 before 8.8.2 allows remote authenticated users to execute arbitrary code because file-upload permissions include the ability to upload a .php file to the main upload directory and/or upload a .php file and a .htaccess file to a subdirectory. Exploitation succeeds only for certain installations with the Apache HTTP Server and the local-storage driver (e.g., when the product was obtained from hub.docker.com).	8.8	More Details
CVE-2021-28355	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28356	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28357	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28358	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28334	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28333	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28332	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28331	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13566	SQL injection vulnerabilities exist in phpGACL 3.3.7. A specially crafted HTTP request can lead to a SQL injection. An attacker can send an HTTP request to trigger this vulnerability In admin/edit_group.php, when the POST parameter action is “Delete”, the POST parameter delete_group leads to a SQL injection.	8.8	More Details
CVE-2020-13568	SQL injection vulnerability exists in phpGACL 3.3.7. A specially crafted HTTP request can lead to a SQL injection. An attacker can send an HTTP request to trigger this vulnerability in admin/edit_group.php, when the POST parameter action is “Submit”, the POST parameter parent_id leads to a SQL injection.	8.8	More Details
CVE-2021-24224	The EFBP_verify_upload_file AJAX action of the Easy Form Builder WordPress plugin through 1.0, available to authenticated users, does not have any security in place to verify uploaded files, allowing low privilege users to upload arbitrary files, leading to RCE.	8.8	More Details
CVE-2021-30147	DMA Softlab Radius Manager 4.4.0 allows CSRF with impacts such as adding new manager accounts via admin.php.	8.8	More Details
CVE-2021-24221	The Quiz And Survey Master – Best Quiz, Exam and Survey Plugin for WordPress plugin before 7.1.12 did not sanitise the result_id GET parameter on pages with the [qsm_result] shortcode without id attribute, concatenating it in a SQL statement and leading to an SQL injection. The lowest role allowed to use this shortcode in post or pages being author, such user could gain unauthorised access to the DBMS. If the shortcode (without the id attribute) is embed on a public page or post, then unauthenticated users could exploit the injection.	8.8	More Details
CVE-2021-24218	The wp_ajax_save_fbe_settings and wp_ajax_delete_fbe_settings AJAX actions of the Facebook for WordPress plugin before 3.0.4 were vulnerable to CSRF due to a lack of nonce protection. The settings in the saveFbeSettings function had no sanitization allowing for script tags to be saved.	8.8	More Details
CVE-2021-29379	An issue was discovered on D-Link DIR-802 A1 devices through 1.00b05. Universal Plug and Play (UPnP) is enabled by default on port 1900. An attacker can perform command injection by injecting a payload into the Search Target (ST) field of the SSDP M-SEARCH discover packet. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	8.8	More Details
CVE-2021-21199	Use after free in Aura in Google Chrome on Linux prior to 89.0.4389.114 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21197	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21196	Heap buffer overflow in TabStrip in Google Chrome on Windows prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21195	Use after free in V8 in Google Chrome prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-21194	Use after free in screen sharing in Google Chrome prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-1362	A vulnerability in the SOAP API endpoint of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, Cisco Unity Connection, and Cisco Prime License Manager could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to improper sanitization of user-supplied input. An attacker could exploit this vulnerability by sending a SOAP API request with crafted parameters to an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges on the underlying Linux operating system of the affected device.	8.8	More Details
CVE-2021-22717	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in C-Bus Toolkit (V1.15.7 and prior) that could allow a remote code execution when processing config files.	8.8	More Details
CVE-2021-22719	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in C-Bus Toolkit (V1.15.7 and prior) that could allow a remote code execution when a file is uploaded.	8.8	More Details
CVE-2020-13592	An exploitable SQL injection vulnerability exists in "global_lists/choices" page of the Rukovoditel Project Management App 2.7.2. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability, this can be done either with administrator credentials or through cross-site request forgery.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13591	An exploitable SQL injection vulnerability exists in the "access_rules/rules_form" page of the Rukovoditel Project Management App 2.7.2. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability, this can be done either with administrator credentials or through cross-site request forgery.	8.8	More Details
CVE-2020-13587	An exploitable SQL injection vulnerability exists in the "forms_fields_rules/rules" page of the Rukovoditel Project Management App 2.7.2. A specially crafted HTTP request can lead to SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability, this can be done either with administrator credentials or through cross-site request forgery.	8.8	More Details
CVE-2021-28327	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28329	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-20687	Cross-site request forgery (CSRF) vulnerability in Kagemai 0.8.8 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	8.8	More Details
CVE-2021-29428	In Gradle before version 7.0, on Unix-like systems, the system temporary directory can be created with open permissions that allow multiple users to create and delete files within it. Gradle builds could be vulnerable to a local privilege escalation from an attacker quickly deleting and recreating files in the system temporary directory. This vulnerability impacted builds using precompiled script plugins written in Kotlin DSL and tests for Gradle plugins written using ProjectBuilder or TestKit. If you are on Windows or modern versions of macOS, you are not vulnerable. If you are on a Unix-like operating system with the "sticky" bit set on your system temporary directory, you are not vulnerable. The problem has been patched and released with Gradle 7.0. As a workaround, on Unix-like operating systems, ensure that the "sticky" bit is set. This only allows the original user (or root) to delete a file. If you are unable to change the permissions of the system temporary directory, you can move the Java temporary directory by setting the System Property `java.io.tmpdir`. The new path needs to limit permissions to the build user only. For additional details refer to the referenced GitHub Security Advisory.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28330	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-28482	Microsoft Exchange Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-23278	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated arbitrary file delete vulnerability induced due to improper input validation at server/maps_srv.js with action removeBackground and server/node_upgrade_srv.js with action removeFirmware. An attacker can send specially crafted packets to delete the files on the system where IPM software is installed.	8.7	More Details
CVE-2021-25374	An improper authorization vulnerability in Samsung Members "samsungrewards" scheme for deeplink in versions 2.4.83.9 in Android O(8.1) and below, and 3.9.00.9 in Android P(9.0) and above allows remote attackers to access a user data related with Samsung Account.	8.6	More Details
CVE-2021-29357	The ECT Provider component in OutSystems Platform Server 10 before 10.0.1104.0 and 11 before 11.9.0 (and LifeTime management console before 11.7.0) allows SSRF for arbitrary outbound HTTP requests.	8.6	More Details
CVE-2020-24136	Directory traversal in Wcms 0.3.2 allows an attacker to read arbitrary files on the server that is running an application via the pagename parameter to wex/html.php.	8.6	More Details
CVE-2021-30480	Zoom Chat through 2021-04-09 on Windows and macOS allows certain remote authenticated attackers to execute arbitrary code without user interaction. An attacker must be within the same organization, or an external party who has been accepted as a contact. NOTE: this is specific to the Zoom Chat software, which is different from the chat feature of the Zoom Meetings and Zoom Video Webinars software.	8.5	More Details
CVE-2021-22190	A path traversal vulnerability via the GitLab Workhorse in all versions of GitLab could result in the leakage of a JWT token	8.5	More Details
CVE-2020-11236	Memory corruption due to invalid value of total dimension in the non-histogram type KPI could lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1892	Memory corruption due to improper input validation while processing IO control which is nonstandard in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Wired Infrastructure and Networking	8.4	More Details
CVE-2021-29440	Grav is a file based Web-platform. Twig processing of static pages can be enabled in the front matter by any administrative user allowed to create or edit pages. As the Twig processor runs unsandboxed, this behavior can be used to gain arbitrary code execution and elevate privileges on the instance. The issue was addressed in version 1.7.11.	8.4	More Details
CVE-2020-11237	Memory crash when accessing histogram type KPI input received due to lack of check of histogram definition before accessing it in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile	8.4	More Details
CVE-2020-11242	User could gain access to secure memory due to incorrect argument into address range validation api used in SDI to capture requested contents in Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details
CVE-2020-11245	Unintended reads and writes by NS EL2 in access control driver due to lack of check of input validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	8.4	More Details
CVE-2020-11234	When sending a socket event message to a user application, invalid information will be passed if socket is freed by other thread resulting in a Use After Free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2020-11246	A double free condition can occur when the device moves to suspend mode during secure playback in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details
CVE-2021-23277	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to unauthenticated eval injection vulnerability. The software does not neutralize code syntax from users before using in the dynamic evaluation call in loadUserFile function under scripts/libs/utils.js. Successful exploitation can allow attackers to control the input to the function and execute attacker controlled commands.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24139	Server-side request forgery in Wcms 0.3.2 lets an attacker send crafted requests from the back-end server of a vulnerable web application via the path parameter to wex/cssjs.php. It can help identify open ports, local network hosts and execute command on local services.	8.3	More Details
CVE-2021-21482	SAP NetWeaver Master Data Management, versions - 710, 710.750, allows a malicious unauthorized user with access to the MDM Server subnet to find the password using a brute force method. If successful, the attacker could obtain access to highly sensitive data and MDM administrative privileges leading to information disclosure vulnerability thereby affecting the confidentiality and integrity of the application. This happens when security guidelines and recommendations concerning administrative accounts of an SAP NetWeaver Master Data Management installation have not been thoroughly reviewed.	8.3	More Details
CVE-2020-24140	Server-side request forgery in Wcms 0.3.2 let an attacker send crafted requests from the back-end server of a vulnerable web application via the pagename parameter to wex/html.php. It can help identify open ports, local network hosts and execute command on local services.	8.3	More Details
CVE-2020-11251	Out-of-bounds read vulnerability while accessing DTMF payload due to lack of check of buffer length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.2	More Details
CVE-2020-11247	Out of bound memory read while unpacking data due to lack of offset length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.2	More Details
CVE-2020-11191	Out of bound read occurs while processing crafted SDP due to lack of check of null string in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	8.2	More Details
CVE-2021-24198	The wpDataTables – Tables & Table Charts premium WordPress plugin before 3.4.2 has Improper Access Control. A low privilege authenticated user that visits the page where the table is published can tamper the parameters to delete the data of another user that are present in the same table through id_key and id_val parameters. By exploiting this issue an attacker is able to delete the data of all users in the same table.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24197	The wpDataTables – Tables & Table Charts premium WordPress plugin before 3.4.2 has Improper Access Control. A low privilege authenticated user that visits the page where the table is published can tamper the parameters to access the data of another user that are present in the same table by taking over the user permissions on the table through formdata[wdt_ID] parameter. By exploiting this issue an attacker is able to access and manage the data of all users in the same table.	8.1	More Details
CVE-2021-28460	Azure Sphere Unsigned Code Execution Vulnerability	8.1	More Details
CVE-2021-28445	Windows Network File System Remote Code Execution Vulnerability	8.1	More Details
CVE-2021-29435	trestle-auth is an authentication plugin for the Trestle admin framework. A vulnerability in trestle-auth versions 0.4.0 and 0.4.1 allows an attacker to create a form that will bypass Rails' built-in CSRF protection when submitted by a victim with a trestle-auth admin session. This potentially allows an attacker to alter protected data, including admin account credentials. The vulnerability has been fixed in trestle-auth 0.4.2 released to RubyGems.	8.1	More Details
CVE-2021-24230	The Jetpack Scan team identified a Cross-Site Request Forgery vulnerability in the Patreon WordPress plugin before 1.7.0, allowing attackers to make a logged in user overwrite or create arbitrary user metadata on the victim’s account once visited. If exploited, this bug can be used to overwrite the “wp_capabilities” meta, which contains the affected user account’s roles and privileges. Doing this would essentially lock them out of the site, blocking them from accessing paid content.	8.1	More Details
CVE-2021-24217	The run_action function of the Facebook for WordPress plugin before 3.0.0 deserializes user supplied data making it possible for PHP objects to be supplied creating an Object Injection vulnerability. There was also a useable magic method in the plugin that could be used to achieve remote code execution.	8.1	More Details
CVE-2020-14104	A RACE CONDITION on XQBACKUP causes a decompression path error on Xiaomi router AX3600 with ROM version =1.0.50.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3460	The Motorola MH702x devices, prior to version 2.0.0.301, do not properly verify the server certificate during communication with the support server which could lead to the communication channel being accessible by an attacker.	8.1	More Details
CVE-2021-21731	A CSRF vulnerability exists in the management page of a ZTE product.The vulnerability is caused because the management page does not fully verify whether the request comes from a trusted user. The attacker could submit a malicious request to the affected device to delete the data. This affects: ZXCLOUD iRAI All versions up to KVM-ProductV6.03.04	8.1	More Details
CVE-2021-29302	TP-Link TL-WR802N(US), Archer_C50v5_US v4_200 <= 2020.06 contains a buffer overflow vulnerability in the httpd process in the body message. The attack vector is: The attacker can get shell of the router by sending a message through the network, which may lead to remote code execution.	8.1	More Details
CVE-2021-23280	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated arbitrary file upload vulnerability. IPM's maps_srv.js allows an attacker to upload a malicious NodeJS file using uploadBackgroud action. An attacker can upload a malicious code or execute any command using a specially crafted packet to exploit the vulnerability.	8.0	More Details
CVE-2021-30481	Valve Steam through 2021-04-10, when a Source engine game is installed, allows remote authenticated users to execute arbitrary code because of a buffer overflow that occurs for a Steam invite after one click.	8.0	More Details
CVE-2021-23279	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to unauthenticated arbitrary file delete vulnerability induced due to improper input validation in meta_driver_srv.js class with saveDriverData action using invalidated driverID. An attacker can send specially crafted packets to delete the files on the system where IPM software is installed.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29427	In Gradle from version 5.1 and before version 7.0 there is a vulnerability which can lead to information disclosure and/or dependency poisoning. Repository content filtering is a security control Gradle introduced to help users specify what repositories are used to resolve specific dependencies. This feature was introduced in the wake of the "A Confusing Dependency" blog post. In some cases, Gradle may ignore content filters and search all repositories for dependencies. This only occurs when repository content filtering is used from within a `pluginManagement` block in a settings file. This may change how dependencies are resolved for Gradle plugins and build scripts. For builds that are vulnerable, there are two risks: 1) Information disclosure: Gradle could make dependency requests to repositories outside your organization and leak internal package identifiers. 2) Dependency poisoning/Dependency confusion: Gradle could download a malicious binary from a repository outside your organization due to name squatting. For a full example and more details refer to the referenced GitHub Security Advisory. The problem has been patched and released with Gradle 7.0. Users relying on this feature should upgrade their build as soon as possible. As a workaround, users may use a company repository which has the right rules for fetching packages from public repositories, or use project level repository content filtering, inside `buildscript.repositories`. This option is available since Gradle 5.1 when the feature was introduced.	8.0	More Details
CVE-2021-0433	In onCreate of DeviceChooserActivity.java, there is a possible way to bypass user consent when pairing a Bluetooth device due to a tapjacking/overlay attack. This could lead to local escalation of privilege and pairing malicious devices with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-171221090	8.0	More Details
CVE-2021-29437	ScratchOAuth2 is an Oauth implementation for Scratch. Any ScratchOAuth2-related data normally accessible and modifiable by a user can be read and modified by a third party. 1. Scratch user visits 3rd party site. 2. 3rd party site asks user for Scratch username. 3. 3rd party site pretends to be user and gets login code from ScratchOAuth2. 4. 3rd party site gives code to user and instructs them to post it on their profile. 5. User posts code on their profile, not knowing it is a ScratchOAuth2 login code. 6. 3rd party site completes login with ScratchOAuth2. 7. 3rd party site has full access to anything the user could do if they directly logged in. See referenced GitHub security advisory for patch notes and workarounds.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25361	An improper access control vulnerability in stickerCenter prior to SMR APR-2021 Release 1 allows local attackers to read or write arbitrary files of system process via untrusted applications.	7.9	More Details
CVE-2021-28322	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-28470	Visual Studio Code GitHub Pull Requests and Issues Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-30184	GNU Chess 6.2.7 allows attackers to execute arbitrary code via crafted PGN (Portable Game Notation) data. This is related to a buffer overflow in the use of a .tmp.epd temporary file in the cmd_pgnload and cmd_pgnreplay functions in frontend/cmd.cc.	7.8	More Details
CVE-2021-28472	Visual Studio Code Maven for Java Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-0445	In start of WelcomeActivity.java, there is a possible residual profile due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-9Android ID: A-172322502	7.8	More Details
CVE-2021-28473	Visual Studio Code Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-28475	Visual Studio Code Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-28471	Remote Development Extension for Visual Studio Code Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-21784	An out-of-bounds write vulnerability exists in the JPG format SOF marker processing of Accusoft ImageGear 19.8. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22718	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in C-Bus Toolkit (V1.15.7 and prior) that could allow a remote code execution when restoring project files.	7.8	More Details
CVE-2021-28454	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-13534	A privilege escalation vulnerability exists in Dream Report 5 R20-2. COM Class Identifiers (CLSID), installed by Dream Report 5 20-2, reference LocalServer32 and InprocServer32 with weak privileges which can lead to privilege escalation when used. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2020-13533	A privilege escalation vulnerability exists in Dream Report 5 R20-2. IIn the default configuration, the following registry keys, which reference binaries with weak permissions, can be abused by attackers to effectively ‘backdoor’ the installation files and escalate privileges when a new user logs in and uses the application.	7.8	More Details
CVE-2020-13532	A privilege escalation vulnerability exists in Dream Report 5 R20-2. In the default configuration, the Syncfusion Dashboard Service service binary can be replaced by attackers to escalate privileges to NT SYSTEM. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2021-22716	A CWE-732: Incorrect Permission Assignment for Critical Resource vulnerability exists that could allow remote code execution when an unprivileged user modifies a file. Affected Product: C-Bus Toolkit (V1.15.9 and prior)	7.8	More Details
CVE-2021-26415	Windows Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-27064	Visual Studio Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-27086	Windows Services and Controller App Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-27088	Windows Event Tracing Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27090	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-28321	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-27091	RPC Endpoint Mapper Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-27095	Windows Media Video Decoder Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27096	NTFS Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-28310	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-28927	The text-to-speech engine in libretro RetroArch for Windows 1.9.0 passes unsanitized input to PowerShell through platform_win32.c via the accessibility_speak_windows function, which allows attackers who have write access on filesystems that are used by RetroArch to execute code via command injection using specially a crafted file and directory names.	7.8	More Details
CVE-2021-28313	Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-28314	Windows Hyper-V Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-28320	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-28315	Windows Media Video Decoder Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27089	Microsoft Internet Messaging API Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-28469	Visual Studio Code Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-28464	VP9 Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-1137	Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or allow an authenticated, local attacker to gain escalated privileges on an affected system. For more information about these vulnerabilities, see the Details section of this advisory.	7.8	More Details
CVE-2021-0429	In pollOnce of ALooper.cpp, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-175074139	7.8	More Details
CVE-2021-0427	In parseExclusiveStateAnnotation of LogEvent.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174488848	7.8	More Details
CVE-2021-28457	Visual Studio Code Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-27486	FATEK Automation WinProladder Versions 3.30 and prior is vulnerable to an integer underflow, which may cause an out-of-bounds write and allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-28436	Windows Speech Runtime Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0426	In parsePrimaryFieldFirstUidAnnotation of LogEvent.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174485572	7.8	More Details
CVE-2021-28685	AsIO2_64.sys and AsIO2_32.sys in ASUS GPUTweak II before 2.3.0.3 allow low-privileged users to interact directly with physical memory (by calling one of several driver routines that map physical memory into the virtual address space of the calling process) and to interact with MSR registers. This could enable low-privileged users to achieve NT AUTHORITY\SYSTEM privileges via a DeviceIoControl.	7.8	More Details
CVE-2020-27228	An incorrect default permissions vulnerability exists in the installation functionality of OpenClinic GA 5.173.3. Overwriting the binary can result in privilege escalation. An attacker can replace a file to exploit this vulnerability.	7.8	More Details
CVE-2020-36313	An issue was discovered in the Linux kernel before 5.7. The KVM subsystem allows out-of-range access to memslots after a deletion, aka CID-0774a964ef56. This affects arch/s390/kvm/kvm-s390.c, include/linux/kvm_host.h, and virt/kvm/kvm_main.c.	7.8	More Details
CVE-2021-1480	Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or allow an authenticated, local attacker to gain escalated privileges on an affected system. For more information about these vulnerabilities, see the Details section of this advisory.	7.8	More Details
CVE-2021-1479	Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or allow an authenticated, local attacker to gain escalated privileges on an affected system. For more information about these vulnerabilities, see the Details section of this advisory.	7.8	More Details
CVE-2021-21545	Dell Peripheral Manager 1.3.1 or greater contains remediation for a local privilege escalation vulnerability that could be potentially exploited to gain arbitrary code execution on the system with privileges of the system user.	7.8	More Details
CVE-2021-28448	Visual Studio Code Kubernetes Tools Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28647	Trend Micro Password Manager version 5 (Consumer) is vulnerable to a DLL Hijacking vulnerability which could allow an attacker to inject a malicious DLL file during the installation progress and could execute a malicious program each time a user installs a program.	7.8	More Details
CVE-2021-28645	An incorrect permission assignment vulnerability in Trend Micro Apex One, Apex One as a Service and OfficeScan XG SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2021-25253	An improper access control vulnerability in Trend Micro Apex One, Trend Micro Apex One as a Service and OfficeScan XG SP1 on a resource used by the service could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2021-28449	Microsoft Office Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-28451	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-25250	An improper access control vulnerability in Trend Micro Apex One, Trend Micro Apex One as a Service and OfficeScan XG SP1 on a sensitive file could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2021-28453	Microsoft Word Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-28458	Azure ms-rest-nodeauth Library Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30463	VestaCP through 0.9.8-24 allows attackers to gain privileges by creating symlinks to files for which they lack permissions. After reading the RKEY value from user.conf under the /usr/local/vesta/data/users/admin directory, the admin password can be changed via a /reset/?action=confirm&user=admin&code= URI. This occurs because chmod is used unsafely.	7.8	More Details
CVE-2021-28466	Raw Image Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-0438	In several functions of InputDispatcher.cpp, WindowManagerService.java, and related files, there is a possible tapjacking attack due to an incorrect FLAG_OBSCURED value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10Android ID: A-152064592	7.8	More Details
CVE-2021-29627	In FreeBSD 13.0-STABLE before n245050, 12.2-STABLE before r369525, 13.0-RC4 before p0, and 12.2-RELEASE before p6, listening socket accept filters implementing the accf_create callback incorrectly freed a process supplied argument string. Additional operations on the socket can lead to a double free or use after free.	7.8	More Details
CVE-2021-0437	In setPlayPolicy of DrmPlugin.cpp, there is a possible double free. This could lead to local escalation of privilege in a privileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-176168330	7.8	More Details
CVE-2021-28468	Raw Image Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-0442	In updateInfo of android_hardware_input_InputApplicationHandle.cpp, there is a possible control of code flow due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174768985	7.8	More Details
CVE-2021-3146	The Dolby Audio X2 (DAX2) API service before 0.8.8.90 on Windows allows local users to gain privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28347	Windows Speech Runtime Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-0439	In setPowerModeWithHandle of com_android_server_power_PowerManagerService.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174243830	7.8	More Details
CVE-2021-28351	Windows Speech Runtime Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-28348	Windows GDI+ Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-28350	Windows GDI+ Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-29154	BPF JIT compilers in the Linux kernel through 5.11.12 have incorrect computation of branch displacements, allowing them to execute arbitrary code within the kernel context. This affects arch/x86/net/bpf_jit_comp.c and arch/x86/net/bpf_jit_comp32.c.	7.8	More Details
CVE-2021-28349	Windows GDI+ Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-26416	Windows Hyper-V Denial of Service Vulnerability	7.7	More Details
CVE-2021-21431	sopel-channelmgnt is a channelmgnt plugin for sopel. In versions prior to 2.0.1, on some IRC servers, restrictions around the removal of the bot using the kick/kickban command could be bypassed when kicking multiple users at once. We also believe it may have been possible to remove users from other channels but due to the wonder that is IRC and following RfCs, We have no POC for that. Freenode is not affected. This is fixed in version 2.0.1. As a workaround, do not use this plugin on networks where TARGMAX > 1.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11243	RRC sends a connection establishment success to NAS even though connection setup validation returns failure and leads to denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile	7.5	More Details
CVE-2020-36317	In the standard library in Rust before 1.49.0, String::retain() function has a panic safety problem. It allows creation of a non-UTF-8 Rust string when the provided closure panics. This bug could result in a memory safety violation when other string APIs assume that UTF-8 encoding is used on the same string.	7.5	More Details
CVE-2020-24285	INTELBRAS TELEFONE IP TIP200 version 60.61.75.22 allows an attacker to obtain sensitive information through /cgi-bin/cgiServer.exx.	7.5	More Details
CVE-2021-0435	In avrc_proc_vendor_command of avrc_api.cc, there is a possible leak of heap data due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174150451	7.5	More Details
CVE-2021-23371	This affects the package chrono-node before 2.2.4. It hangs on a date-like string with lots of embedded spaces.	7.5	More Details
CVE-2021-0431	In avrc_msg_cback of avrc_api.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a paired device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174149901	7.5	More Details
CVE-2021-28878	In the standard library in Rust before 1.52.0, the Zip implementation calls __iterator_get_unchecked() more than once for the same index (under certain conditions) when next_back() and next() are used together. This bug could lead to a memory safety violation due to an unmet safety requirement for the TrustedRandomAccess trait.	7.5	More Details
CVE-2015-20001	In the standard library in Rust before 1.2.0, BinaryHeap is not panic-safe. The binary heap is left in an inconsistent state when the comparison of generic elements inside sift_up or sift_down_range panics. This bug leads to a drop of zeroed memory as an arbitrary type, which can result in a memory safety violation.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28875	In the standard library in Rust before 1.50.0, read_to_end() does not validate the return value from Read in an unsafe context. This bug could lead to a buffer overflow.	7.5	More Details
CVE-2021-28877	In the standard library in Rust before 1.51.0, the Zip implementation calls __iterator_get_unchecked() for the same index more than once when nested. This bug can lead to a memory safety violation due to an unmet safety requirement for the TrustedRandomAccess trait.	7.5	More Details
CVE-2019-15059	In Liberty lisPBX 2.0-4, configuration backup files can be retrieved remotely from /backup/lispbx-CONF-YYYY-MM-DD.tar or /backup/lispbx-CDR-YYYY-MM-DD.tar without authentication or authorization. These configuration files have all PBX information including extension numbers, contacts, and passwords.	7.5	More Details
CVE-2021-3128	In ASUS RT-AX3000, ZenWiFi AX (XT8), RT-AX88U, and other ASUS routers with firmware < 3.0.0.4.386.42095 or < 9.0.0.4.386.41994, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set.	7.5	More Details
CVE-2021-3125	In TP-Link TL-XDR3230 < 1.0.12, TL-XDR1850 < 1.0.9, TL-XDR1860 < 1.0.14, TL-XDR3250 < 1.0.2, TL-XDR6060 Turbo < 1.1.8, TL-XDR5430 < 1.0.11, and possibly others, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set.	7.5	More Details
CVE-2021-23370	This affects the package swiper before 6.5.1.	7.5	More Details
CVE-2020-4965	IBM Jazz Team Server products use weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 192422.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23270	In Gargoyle OS 1.12.0, when IPv6 is used, a routing loop can occur that generates excessive network traffic between an affected device and its upstream ISP's router. This occurs when a link prefix route points to a point-to-point link, a destination IPv6 address belongs to the prefix and is not a local IPv6 address, and a router advertisement is received with at least one global unique IPv6 prefix for which the on-link flag is set.	7.5	More Details
CVE-2021-24227	The Jetpack Scan team identified a Local File Disclosure vulnerability in the Patreon WordPress plugin before 1.7.0 that could be abused by anyone visiting the site. Using this attack vector, an attacker could leak important internal files like wp-config.php, which contains database credentials and cryptographic keys used in the generation of nonces and cookies.	7.5	More Details
CVE-2021-24226	In the AccessAlly WordPress plugin before 3.5.7, the file "resource/frontend/product/product-shortcode.php" responsible for the [accessally_order_form] shortcode is dumping serialize($_SERVER), which contains all environment variables. The leakage occurs on all public facing pages containing the [accessally_order_form] shortcode, no login or administrator role is required.	7.5	More Details
CVE-2021-29262	When starting Apache Solr versions prior to 8.8.2, configured with the SaslZkACLProvider or VMParamsAllAndReadonlyDigestZkACLProvider and no existing security.json znode, if the optional read-only user is configured then Solr would not treat that node as a sensitive path and would allow it to be readable. Additionally, with any ZkACLProvider, if the security.json is already present, Solr will not automatically update the ACLs.	7.5	More Details
CVE-2021-30185	CERN Indico before 2.3.4 can use an attacker-supplied Host header in a password reset link.	7.5	More Details
CVE-2021-1252	A vulnerability in the Excel XLM macro parsing module in Clam AntiVirus (ClamAV) Software versions 0.103.0 and 0.103.1 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to improper error handling that may result in an infinite loop. An attacker could exploit this vulnerability by sending a crafted Excel file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process hang, resulting in a denial of service condition.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25584	In FreeBSD 13.0-STABLE before n245118, 12.2-STABLE before r369552, 11.4-STABLE before r369560, 13.0-RC5 before p1, 12.2-RELEASE before p6, and 11.4-RELEASE before p9, a superuser inside a FreeBSD jail configured with the non-default allow.mount permission could cause a race condition between the lookup of ".." and remounting a filesystem, allowing access to filesystem hierarchy outside of the jail.	7.5	More Details
CVE-2021-28439	Windows TCP/IP Driver Denial of Service Vulnerability	7.5	More Details
CVE-2021-1405	A vulnerability in the email parsing module in Clam AntiVirus (ClamAV) Software version 0.103.1 and all prior versions could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to improper variable initialization that may result in an NULL pointer read. An attacker could exploit this vulnerability by sending a crafted email to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition.	7.5	More Details
CVE-2021-28319	Windows TCP/IP Driver Denial of Service Vulnerability	7.5	More Details
CVE-2020-11255	Denial of service while processing RTCP packets containing multiple SDES reports due to memory for last SDES packet is freed and rest of the memory is leaked in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables	7.5	More Details
CVE-2021-1404	A vulnerability in the PDF parsing module in Clam AntiVirus (ClamAV) Software versions 0.103.0 and 0.103.1 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to improper buffer size tracking that may result in a heap buffer over-read. An attacker could exploit this vulnerability by sending a crafted PDF file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process to crash, resulting in a denial of service condition.	7.5	More Details
CVE-2020-23539	An issue was discovered in Realtek rtl8723de BLE Stack <= 4.1 that allows remote attackers to cause a Denial of Service via the interval field to the CONNECT_REQ message.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21432	Vela is a Pipeline Automation (CI/CD) framework built on Linux container technology written in Golang. An authentication mechanism added in version 0.7.0 enables some malicious user to obtain secrets utilizing the injected credentials within the `~/.netrc` file. Refer to the referenced GitHub Security Advisory for complete details. This is fixed in version 0.7.5.	7.5	More Details
CVE-2020-14099	On Xiaomi router AX1800 rom version < 1.0.336 and RM1800 root version < 1.0.26, the encryption scheme for a user's backup files uses hard-coded keys, which can expose sensitive information such as a user's password.	7.5	More Details
CVE-2021-28324	Windows SMB Information Disclosure Vulnerability	7.5	More Details
CVE-2021-3328	An issue was discovered in Aprelium Abyss Web Server X1 2.12.1 and 2.14. A crafted HTTP request can lead to an out-of-bounds read that crashes the application.	7.5	More Details
CVE-2020-6590	Forcepoint Web Security Content Gateway versions prior to 8.5.4 improperly process XML input, leading to information disclosure.	7.5	More Details
CVE-2021-1308	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	7.4	More Details
CVE-2021-1251	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1309	Multiple vulnerabilities exist in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Small Business RV Series Routers. An unauthenticated, adjacent attacker could execute arbitrary code or cause an affected router to leak system memory or reload. A memory leak or device reload would cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	7.4	More Details
CVE-2021-21198	Out of bounds read in IPC in Google Chrome prior to 89.0.4389.114 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	7.4	More Details
CVE-2021-0446	In ImportVCardActivity, there is a possible way to bypass user consent due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172252122	7.3	More Details
CVE-2021-30462	VestaCP through 0.9.8-24 allows the admin user to escalate privileges to root because the Sudo configuration does not require a password to run /usr/local/vesta/bin scripts.	7.2	More Details
CVE-2021-29439	The Grav admin plugin prior to version 1.10.11 does not correctly verify caller's privileges. As a consequence, users with the permission `admin.login` can install third-party plugins and their dependencies. By installing the right plugin, an attacker can obtain an arbitrary code execution primitive and elevate their privileges on the instance. The vulnerability has been addressed in version 1.10.11. As a mitigation blocking access to the `/admin` path from untrusted sources will reduce the probability of exploitation.	7.2	More Details
CVE-2021-20022	SonicWall Email Security version 10.0.9.x contains a vulnerability that allows a post-authenticated attacker to upload an arbitrary file to the remote host.	7.2	More Details
CVE-2020-11252	Trustzone initialization code will disable xPU`s when memory dumps are enabled and lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.2	More Details
CVE-2021-22720	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in C-Bus Toolkit (V1.15.7 and prior) that could allow a remote code execution when restoring a project.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28446	Windows Portmapping Information Disclosure Vulnerability	7.1	More Details
CVE-2021-28452	Microsoft Outlook Memory Corruption Vulnerability	7.1	More Details
CVE-2021-25356	An improper caller check vulnerability in Managed Provisioning prior to SMR APR-2021 Release 1 allows unprivileged application to install arbitrary application, grant device admin permission and then delete several installed application.	7.1	More Details
CVE-2021-20692	Directory traversal vulnerability in Archive collectively operation utility Ver.2.10.1.0 and earlier allows an attacker to create or overwrite files by leading a user to expand a malicious ZIP archives.	7.1	More Details
CVE-2021-23276	Eaton Intelligent Power Manager (IPM) prior to 1.69 is vulnerable to authenticated SQL injection. A malicious user can send a specially crafted packet to exploit the vulnerability. Successful exploitation of this vulnerability can allow attackers to add users in the data base.	7.1	More Details
CVE-2021-0432	In ClearPullerCacheIfNecessary and ForceClearPullerCache of StatsPullerManager.cpp, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-173552790	7.0	More Details
CVE-2021-28440	Windows Installer Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-1386	A vulnerability in the dynamic link library (DLL) loading mechanism in Cisco Advanced Malware Protection (AMP) for Endpoints Windows Connector, ClamAV for Windows, and Immunet could allow an authenticated, local attacker to perform a DLL hijacking attack on an affected Windows system. To exploit this vulnerability, the attacker would need valid credentials on the system. The vulnerability is due to insufficient validation of directory search paths at run time. An attacker could exploit this vulnerability by placing a malicious DLL file on an affected system. A successful exploit could allow the attacker to execute arbitrary code with SYSTEM privileges.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29221	A local privilege escalation vulnerability was discovered in Erlang/OTP prior to version 23.2.3. By adding files to an existing installation's directory, a local attacker could hijack accounts of other users running Erlang programs or possibly coerce a service running with "erlsrv.exe" to execute arbitrary code as Local System. This can occur only under specific conditions on Windows with unsafe filesystem permissions.	7.0	More Details
CVE-2021-28477	Visual Studio Code Remote Code Execution Vulnerability	7.0	More Details
CVE-2021-27072	Win32k Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-25362	An improper permission management in CertInstaller prior to SMR APR-2021 Release 1 allows untrusted applications to delete certain local files.	6.8	More Details
CVE-2021-25363	An improper access control in ActivityManagerService prior to SMR APR-2021 Release 1 allows untrusted applications to access running processesdelete some local files.	6.8	More Details
CVE-2021-27092	Azure AD Web Sign-in Security Feature Bypass Vulnerability	6.8	More Details
CVE-2020-11231	Two threads call one or both functions concurrently leading to corruption of pointers and reference counters which in turn can lead to heap corruption in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	6.7	More Details
CVE-2021-1485	A vulnerability in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges on the underlying Linux operating system (OS) of an affected device. This vulnerability is due to insufficient input validation of commands that are supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to an affected command. A successful exploit could allow the attacker to execute commands on the underlying Linux OS with root privileges.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0468	In LK, there is a possible escalation of privilege due to an insecure default value. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-180427272	6.6	More Details
CVE-2021-1474	Multiple vulnerabilities in the Admin audit log export feature and Scheduled Reports feature of Cisco Umbrella could allow an authenticated, remote attacker to perform formula and link injection attacks on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2021-1475	Multiple vulnerabilities in the Admin audit log export feature and Scheduled Reports feature of Cisco Umbrella could allow an authenticated, remote attacker to perform formula and link injection attacks on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	6.5	More Details
CVE-2021-28174	Mitake smart stock selection system contains a broken authentication vulnerability. By manipulating the parameters in the URL, remote attackers can gain the privileged permissions to access transaction record, and fraudulent trading without login.	6.5	More Details
CVE-2021-20480	IBM WebSphere Application Server 7.0, 8.0, and 8.5 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197502.	6.5	More Details
CVE-2021-27603	An RFC enabled function module SPI_WAIT_MILLIS in SAP NetWeaver AS ABAP, versions - 731, 740, 750, allows to keep a work process busy for any length of time. An attacker could call this function module multiple times to block all work processes thereby causing Denial of Service and affecting the Availability of the SAP system.	6.5	More Details
CVE-2021-25375	Using predictable index for attachments in Samsung Email prior to version 6.1.41.0 allows remote attackers to get attachments of another emails when users open the malicious attachment.	6.5	More Details
CVE-2021-21485	An unauthorized attacker may be able to entice an administrator to invoke telnet commands of an SAP NetWeaver Application Server for Java that allow the attacker to gain NTLM hashes of a privileged user.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21729	Some ZTE products have CSRF vulnerability. Because some pages lack CSRF random value verification, attackers could perform illegal authorization operations by constructing messages.This affects: ZXHN H168N V3.5.0_EG1T5_TE, V2.5.5, ZXHN H108N V2.5.5_BTMT1	6.5	More Details
CVE-2021-27609	SAP Focused RUN versions 200, 300, does not perform necessary authorization checks for an authenticated user, which allows a user to call the oData service and manipulate the activation for the SAP EarlyWatch Alert service data collection and sending to SAP without the intended authorization.	6.5	More Details
CVE-2020-28590	An out-of-bounds read vulnerability exists in the Obj File TriangleMesh::TriangleMesh() functionality of Slic3r libslic3r 1.3.0 and Master Commit 92abbc42. A specially crafted obj file could lead to information disclosure. An attacker can provide a malicious file to trigger this vulnerability.	6.5	More Details
CVE-2021-30112	Web-School ERP V 5.0 contains a cross-site request forgery (CSRF) vulnerability that allows a remote attacker to create a student_leave_application request through module/core/studentleaveapplication/create. The application fails to validate the CSRF token for a POST request using Guardian privilege.	6.5	More Details
CVE-2021-28441	Windows Hyper-V Information Disclosure Vulnerability	6.5	More Details
CVE-2021-28442	Windows TCP/IP Information Disclosure Vulnerability	6.5	More Details
CVE-2021-30114	Web-School ERP V 5.0 contains a cross-site request forgery (CSRF) vulnerability that allows a remote attacker to create a voucher payment request through module/accounting/voucher/create. The application fails to validate the CSRF token for a POST request using admin privilege.	6.5	More Details
CVE-2021-24199	The wpDataTables – Tables & Table Charts premium WordPress plugin before 3.4.2 allows a low privilege authenticated user to perform Boolean-based blind SQL Injection in the table list page on the endpoint /wp-admin/admin-ajax.php?action=get_wdtable&table_id=1, on the 'start' HTTP POST parameter. This allows an attacker to access all the data in the database and obtain access to the WordPress application.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25327	Skyworth Digital Technology RN510 V.3.1.0.4 contains a cross-site request forgery (CSRF) vulnerability in /cgi-bin/net-routeadd.asp and /cgi-bin/sec-urlfilter.asp. Missing CSRF protection in devices can lead to XSRF, as the above pages are vulnerable to cross-site scripting (XSS).	6.5	More Details
CVE-2021-22312	There is a memory leak vulnerability in some Huawei products. An authenticated remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause some service abnormal. Affected product include some versions of IPS Module, NGFW Module, Secospace USG6300, Secospace USG6500, Secospace USG6600 and USG9500.	6.5	More Details
CVE-2021-28166	In Eclipse Mosquitto version 2.0.0 to 2.0.9, if an authenticated client that had connected with MQTT v5 sent a crafted CONNACK message to the broker, a NULL pointer dereference would occur.	6.5	More Details
CVE-2021-3482	A flaw was found in Exiv2 in versions before and including 0.27.4-RC1. Improper input validation of the rawData.size property in Jp2Image::readMetadata() in jp2image.cpp can lead to a heap-based buffer overflow via a crafted JPG image containing malicious EXIF data.	6.5	More Details
CVE-2021-22513	Missing Authorization vulnerability in Micro Focus Application Automation Tools Plugin - Jenkins plugin. The vulnerability affects version 6.7 and earlier versions. The vulnerability could allow access without permission checks.	6.5	More Details
CVE-2021-22512	Cross-Site Request Forgery (CSRF) vulnerability in Micro Focus Application Automation Tools Plugin - Jenkins plugin. The vulnerability affects version 6.7 and earlier versions. The vulnerability could allow form validation without permission checks.	6.5	More Details
CVE-2021-24200	The wpDataTables – Tables & Table Charts premium WordPress plugin before 3.4.2 allows a low privilege authenticated user to perform Boolean-based blind SQL Injection in the table list page on the endpoint /wp-admin/admin-ajax.php?action=get_wdtable&table_id=1, on the 'length' HTTP POST parameter. This allows an attacker to access all the data in the database and obtain access to the WordPress application.	6.5	More Details
CVE-2021-27067	Azure DevOps Server and Team Foundation Server Information Disclosure Vulnerability	6.5	More Details
CVE-2021-28328	Windows DNS Information Disclosure Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22511	Improper Certificate Validation vulnerability in Micro Focus Application Automation Tools Plugin - Jenkins plugin. The vulnerability affects version 6.7 and earlier versions. The vulnerability could allow unconditionally disabling of SSL/TLS certificates.	6.5	More Details
CVE-2021-28325	Windows SMB Information Disclosure Vulnerability	6.5	More Details
CVE-2021-22115	Cloud Controller API versions prior to 1.106.0 logs service broker credentials if the default value of db logging config field is changed. CAPI database logs service broker password in plain text whenever a job to clean up orphaned items is run by Cloud Controller.	6.5	More Details
CVE-2021-30485	An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_internal_dtd(), while parsing a crafted XML file, performs incorrect memory handling, leading to a NULL pointer dereference while running strcmp() on a NULL pointer.	6.5	More Details
CVE-2021-28323	Windows DNS Information Disclosure Vulnerability	6.5	More Details
CVE-2021-28311	Windows Application Compatibility Cache Denial of Service Vulnerability	6.5	More Details
CVE-2021-24231	The Jetpack Scan team identified a Cross-Site Request Forgery vulnerability in the Patreon WordPress plugin before 1.7.0, allowing attackers to make a logged administrator disconnect the site from Patreon by visiting a specially crafted link.	6.5	More Details
CVE-2021-3413	A flaw was found in Red Hat Satellite in tfm-rubygem-foreman_azure_rm in versions before 2.2.0. A credential leak was identified which will expose Azure Resource Manager's secret key through JSON of the API output. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1415	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.	6.3	More Details
CVE-2021-1414	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.	6.3	More Details
CVE-2021-1413	Multiple vulnerabilities in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code with elevated privileges equivalent to the web service process on an affected device. These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device.	6.3	More Details
CVE-2021-21392	Synapse is a Matrix reference homeserver written in python (pypi package matrix-synapse). Matrix is an ecosystem for open federated Instant Messaging and VoIP. In Synapse before version 1.28.0 requests to user provided domains were not restricted to external IP addresses when transitional IPv6 addresses were used. Outbound requests to federation, identity servers, when calculating the key validity for third-party invite events, sending push notifications, and generating URL previews are affected. This could cause Synapse to make requests to internal infrastructure on dual-stack networks. See referenced GitHub security advisory for details and workarounds.	6.3	More Details
CVE-2021-26413	Windows Installer Spoofing Vulnerability	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28459	Azure DevOps Server Spoofing Vulnerability	6.1	More Details
CVE-2021-29370	A UXSS was discovered in the Thanos-Soft Cheetah Browser in Android 1.2.0 due to the inadequate filter of the intent scheme. This resulted in Cross-site scripting on the cheetah browser in any website.	6.1	More Details
CVE-2021-1380	Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against an interface user. These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading an interface user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.	6.1	More Details
CVE-2021-1409	Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against an interface user. These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading an interface user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1408	Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against an interface user. These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading an interface user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.	6.1	More Details
CVE-2021-1407	Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against an interface user. These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by persuading an interface user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.	6.1	More Details
CVE-2021-1463	A vulnerability in the web-based management interface of Cisco Unified Intelligence Center Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2021-22510	Reflected XSS vulnerability in Micro Focus Application Automation Tools Plugin - Jenkins plugin. The vulnerability affects all version 6.7 and earlier versions.	6.1	More Details
CVE-2021-25926	In SiCKRAGE, versions 9.3.54.dev1 to 10.0.11.dev1 are vulnerable to Reflected Cross-Site-Scripting (XSS) due to user input not being validated properly in the `quicksearch` feature. Therefore, an attacker can steal a user's sessionID to masquerade as a victim user, to carry out any actions in the context of the user.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30458	An issue was discovered in Wikimedia Parsoid before 0.11.1 and 0.12.x before 0.12.2. An attacker can send crafted wikitext that Utils/WTUtils.php will transform by using a <meta> tag, bypassing sanitization steps, and potentially allowing for XSS.	6.1	More Details
CVE-2020-24135	A Reflected Cross Site Scripting (XSS) Vulnerability was discovered in Wcms 0.3.2, which allows remote attackers to inject arbitrary web script and HTML via the type parameter to wex/cssjs.php.	6.1	More Details
CVE-2021-20080	Insufficient output sanitization in ManageEngine ServiceDesk Plus before version 11200 and ManageEngine AssetExplorer before version 6800 allows a remote, unauthenticated attacker to conduct persistent cross-site scripting (XSS) attacks by uploading a crafted XML asset file.	6.1	More Details
CVE-2020-24138	Cross Site Scripting (XSS) vulnerability in wcms 0.3.2 allows remote attackers to inject arbitrary web script and HTML via the pagename parameter to wex/html.php.	6.1	More Details
CVE-2021-20691	Cross-site scripting vulnerability in Yomi-Search Ver4.22 allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-20690	Cross-site scripting vulnerability in Yomi-Search Ver4.22 allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-27945	The Squirro Insights Engine was affected by a Reflected Cross-Site Scripting (XSS) vulnerability affecting versions 2.0.0 up to and including 3.2.4. An attacker can use the vulnerability to inject malicious JavaScript code into the application, which will execute within the browser of any user who views the relevant application content. The attacker-supplied code can perform a wide variety of actions, such as stealing victims' session tokens or login credentials, performing arbitrary actions on their behalf, and logging their keystrokes.	6.1	More Details
CVE-2021-20689	Cross-site scripting vulnerability in Yomi-Search Ver4.22 allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-3163	A vulnerability in the HTML editor of Slab Quill 4.8.0 allows an attacker to execute arbitrary JavaScript by storing an XSS payload (a crafted onloadstart attribute of an IMG element) in a text field. Note: Researchers have claimed that this issue is not within the product itself, but is intended behavior in a web browser	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20688	Cross-site scripting vulnerability in Click Ranker Ver.3.5 allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-20686	Cross-site scripting vulnerability in Kagemai 0.8.8 allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-24213	The GiveWP – Donation Plugin and Fundraising Platform WordPress plugin before 2.10.0 was affected by a reflected Cross-Site Scripting vulnerability inside of the administration panel, via the 's' GET parameter on the Donors page.	6.1	More Details
CVE-2021-20685	Cross-site scripting vulnerability in Kagemai 0.8.8 allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2021-20684	Cross-site scripting vulnerability in MagazinegerZ v.1.01 allows remote attackers to inject an arbitrary script via unspecified vectors.	6.1	More Details
CVE-2020-23761	Cross Site Scripting (XSS) vulnerability in subrion CMS Version <= 4.2.1 allows remote attackers to execute arbitrary web script via the "payment gateway" column on transactions tab.	6.1	More Details
CVE-2021-28924	Self Authenticated XSS in Nagios Network Analyzer before 2.4.2 via the nagiosna/groups/queries page.	6.1	More Details
CVE-2021-30113	A blind XSS vulnerability exists in Web-School ERP V 5.0 via (Add Events) in event name and description fields. An attacker can inject a JavaScript code that will be stored in the page. If any visitor sees the event, then the payload will be executed and sends the victim's information to the attacker website.	6.1	More Details
CVE-2021-25365	An improper exception control in softsimd prior to SMR APR-2021 Release 1 allows unprivileged applications to access the API in softsimd.	5.9	More Details
CVE-2021-25380	Improper handling of exceptional conditions in Bixby prior to version 3.0.53.02 allows attacker to execute the actions registered by the user.	5.8	More Details
CVE-2021-28444	Windows Hyper-V Security Feature Bypass Vulnerability	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27079	Windows Media Photo Codec Information Disclosure Vulnerability	5.7	More Details
CVE-2021-25357	A pendingIntent hijacking vulnerability in Create Movie prior to SMR APR-2021 Release 1 in Android O(8.x) and P(9.0), 3.4.81.1 in Android Q(10,0), and 3.6.80.7 in Android R(11.0) allows unprivileged applications to access contact information.	5.6	More Details
CVE-2021-23369	The package handlebars before 4.7.7 are vulnerable to Remote Code Execution (RCE) when selecting certain compiling options to compile templates coming from an untrusted source.	5.6	More Details
CVE-2020-14106	The application in the mobile phone can unauthorized access to the list of running processes in the mobile phone, Xiaomi Mobile Phone MIUI < 2021.01.26.	5.5	More Details
CVE-2021-28326	Windows AppX Deployment Server Denial of Service Vulnerability	5.5	More Details
CVE-2021-25373	Using unsafe PendingIntent in Customization Service prior to version 2.2.02.1 in Android O(8.x), 2.4.03.0 in Android P(9.0), 2.7.02.1 in Android Q(10.0) and 2.9.01.1 in Android R(11.0) allows local attackers to perform unauthorized action without permission via hijacking the PendingIntent.	5.5	More Details
CVE-2020-14103	The application in the mobile phone can read the SNO information of the device, Xiaomi 10 MIUI < 2020.01.15.	5.5	More Details
CVE-2021-28318	Windows GDI+ Information Disclosure Vulnerability	5.5	More Details
CVE-2021-28317	Microsoft Windows Codecs Library Information Disclosure Vulnerability	5.5	More Details
CVE-2021-28309	Windows Kernel Information Disclosure Vulnerability	5.5	More Details
CVE-2021-27093	Windows Kernel Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28435	Windows Event Tracing Information Disclosure Vulnerability	5.5	More Details
CVE-2021-0471	In decrypt_1_2 of CryptoPlugin.cpp, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-176444786	5.5	More Details
CVE-2020-36310	An issue was discovered in the Linux kernel before 5.8. arch/x86/kvm/svm/svm.c allows a set_memory_region_test infinite loop for certain nested page faults, aka CID-e72436bc3a52.	5.5	More Details
CVE-2021-25381	Using unsafe PendingIntent in Samsung Account in versions 10.8.0.4 in Android P(9.0) and below, and 12.1.1.3 in Android Q(10.0) and above allows local attackers to perform unauthorized action without permission via hijacking the PendingIntent.	5.5	More Details
CVE-2020-15734	An Origin Validation Error vulnerability in Bitdefender Safepay allows an attacker to manipulate the browser's file upload capability into accessing other files in the same directory or sub-directories. This issue affects: Bitdefender Safepay versions prior to 25.0.7.29.	5.5	More Details
CVE-2021-3462	A privilege escalation vulnerability in Lenovo Power Management Driver for Windows 10, prior to version 1.67.17.54, that could allow unauthorized access to the driver's device object.	5.5	More Details
CVE-2020-36312	An issue was discovered in the Linux kernel before 5.8.10. virt/kvm/kvm_main.c has a kvm_io_bus_unregister_dev memory leak upon a kmalloc failure, aka CID-f65886606c2d.	5.5	More Details
CVE-2021-30178	An issue was discovered in the Linux kernel through 5.11.11. synic_get in arch/x86/kvm/hyperv.c has a NULL pointer dereference for certain accesses to the SynIC Hyper-V context, aka CID-919f4ebc5987.	5.5	More Details
CVE-2021-28646	An insecure file permissions vulnerability in Trend Micro Apex One, Apex One as a Service and OfficeScan XG SP1 could allow a local attacker to take control of a specific log file on affected installations.	5.5	More Details
CVE-2020-36311	An issue was discovered in the Linux kernel before 5.9. arch/x86/kvm/svm/sev.c allows attackers to cause a denial of service (soft lockup) by triggering destruction of a large SEV VM (which requires unregistering many encrypted regions), aka CID-7be74942f184.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29626	In FreeBSD 13.0-STABLE before n245117, 12.2-STABLE before r369551, 11.4-STABLE before r369559, 13.0-RC5 before p1, 12.2-RELEASE before p6, and 11.4-RELEASE before p9, copy-on-write logic failed to invalidate shared memory page mappings between multiple processes allowing an unprivileged process to maintain a mapping after it is freed, allowing the process to read private data belonging to other processes or the kernel.	5.5	More Details
CVE-2020-36316	In RELIC before 2021-04-03, there is a buffer overflow in PKCS#1 v1.5 signature verification because garbage bytes can be present.	5.5	More Details
CVE-2021-28456	Microsoft Excel Information Disclosure Vulnerability	5.5	More Details
CVE-2021-28437	Windows Installer Information Disclosure Vulnerability	5.5	More Details
CVE-2021-0436	In CryptoPlugin::decrypt of CryptoPlugin.cpp, there is a possible out of bounds read due to integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-176496160	5.5	More Details
CVE-2021-0400	In injectBestLocation and handleUpdateLocation of GnssLocationProvider.java, there is a possible incorrect reporting of location data to emergency services due to improper input validation. This could lead to incorrect reporting of location data to emergency services with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11Android ID: A-177561690	5.5	More Details
CVE-2021-0428	In getSimSerialNumber of TelephonyManager.java, there is a possible way to read a trackable identifier due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-173421434	5.5	More Details
CVE-2021-28443	Windows Console Driver Denial of Service Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26417	Windows Overlay Filter Information Disclosure Vulnerability	5.5	More Details
CVE-2021-28686	AsIO2_64.sys and AsIO2_32.sys in ASUS GPUTweak II before 2.3.0.3 allow low-privileged users to trigger a stack-based buffer overflow. This could enable low-privileged users to achieve Denial of Service via a DeviceIoControl.	5.5	More Details
CVE-2021-28438	Windows Console Driver Denial of Service Vulnerability	5.5	More Details
CVE-2021-0444	In onActivityResult of QuickContactActivity.java, there is an unnecessary return of an intent. This could lead to local information disclosure of contact data with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-178825358	5.5	More Details
CVE-2021-25326	Skyworth Digital Technology RN510 V.3.1.0.4 is affected by an incorrect access control vulnerability in/cgi-bin/test_version.asp. If Wi-Fi is connected but an unauthenticated user visits a URL, the SSID password and web UI password may be disclosed.	5.4	More Details
CVE-2021-3012	A cross-site scripting (XSS) vulnerability in the Document Link of documents in ESRI Enterprise before 10.9 allows remote authenticated users to inject arbitrary JavaScript code via a malicious HTML attribute such as onerror (in the URL field of the Parameters tab).	5.4	More Details
CVE-2021-29436	Anuko Time Tracker is an open source, web-based time tracking application written in PHP. In Time Tracker before version 1.19.27.5431 a Cross site request forgery (CSRF) vulnerability existed. The nature of CSRF is that a logged on user may be tricked by social engineering to click on an attacker-provided form that executes an unintended action such as changing user password. The vulnerability is fixed in Time Tracker version 1.19.27.5431. Upgrade is recommended. If upgrade is not practical, introduce ttMitigateCSRF() function in /WEB-INF/lib/common.php.lib using the latest available code and call it from ttAccessAllowed().	5.4	More Details
CVE-2021-30111	A stored XSS vulnerability exists in Web-School ERP V 5.0 via (Add Events) in the event name and description fields. An attack can inject a JavaScript code that will be stored in the page. If any visitor sees the events, then the payload will be executed.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30039	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the "Fever" or "Blood Pressure" field on the patients/register-report.php.	5.4	More Details
CVE-2021-30034	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the Symptons field on patients/register-report.php.	5.4	More Details
CVE-2019-17656	A Stack-based Buffer Overflow vulnerability in the HTTPD daemon of FortiOS 6.0.10 and below, 6.2.2 and below and FortiProxy 1.0.x, 1.1.x, 1.2.9 and below, 2.0.0 and below may allow an authenticated remote attacker to crash the service by sending a malformed PUT request to the server. Fortinet is not aware of any successful exploitation of this vulnerability that would lead to code execution.	5.4	More Details
CVE-2021-20519	IBM Jazz Team Server products are 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: 198441.	5.4	More Details
CVE-2020-23762	Cross Site Scripting (XSS) vulnerability in the Larsens Calender plugin Version <= 1.2 for WordPress allows remote attackers to execute arbitrary web script via the "titel" column on the "Eintrage hinzufugen" tab.	5.4	More Details
CVE-2021-24225	The Advanced Booking Calendar WordPress plugin before 1.6.7 did not sanitise the calId GET parameter in the "Seasons & Calendars" page before outputing it in an A tag, leading to a reflected XSS issue	5.4	More Details
CVE-2021-25925	in SiCKRAGE, versions 4.2.0 to 10.0.11.dev1 are vulnerable to Stored Cross-Site-Scripting (XSS) due to user input not being validated properly when processed by the server. Therefore, an attacker can inject arbitrary JavaScript code inside the application, and possibly steal a user's sensitive information.	5.4	More Details
CVE-2021-27601	SAP NetWeaver AS Java (Applications based on HTMLB for Java) allows a basic-level authorized attacker to store a malicious file on the server. When a victim tries to open this file, it results in a Cross-Site Scripting (XSS) vulnerability and the attacker can read and modify data. However, the attacker does not have control over kind or degree.	5.4	More Details
CVE-2020-4920	IBM Jazz Team Server products are vulnerable to stored 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: 191396.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27600	SAP Manufacturing Execution (System Rules), versions - 15.1, 15.2, 15.3, 15.4, allows an authorized attacker to embed malicious code into HTTP parameter and send it to the server because SAP Manufacturing Execution (System Rules) tab does not sufficiently encode some parameters, resulting in Stored Cross-Site Scripting (XSS) vulnerability. The malicious code can be used for different purposes. e.g., information can be read, modified, and sent to the attacker. However, availability of the server cannot be impacted.	5.4	More Details
CVE-2021-30030	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the Full Name field on register-patient.php.	5.4	More Details
CVE-2021-30637	htmly 2.8.0 allows stored XSS via the blog title, Tagline, or Description to config.html.php.	5.4	More Details
CVE-2021-30044	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the First Name or Last Name field on staff/register.php.	5.4	More Details
CVE-2021-30042	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the "Clinic Name", "Clinic Address", "Clinic City", or "Clinic Contact" field on clinics/register.php	5.4	More Details
CVE-2021-21394	Synapse is a Matrix reference homeserver written in python (pypi package matrix-synapse). Matrix is an ecosystem for open federated Instant Messaging and VoIP. In Synapse before version 1.28.0 Synapse is missing input validation of some parameters on the endpoints used to confirm third-party identifiers could cause excessive use of disk space and memory leading to resource exhaustion. Note that the groups feature is not part of the Matrix specification and the chosen maximum lengths are arbitrary. Not all clients might abide by them. Refer to referenced GitHub security advisory for additional details including workarounds.	5.3	More Details
CVE-2021-21393	Synapse is a Matrix reference homeserver written in python (pypi package matrix-synapse). Matrix is an ecosystem for open federated Instant Messaging and VoIP. In Synapse before version 1.28.0 Synapse is missing input validation of some parameters on the endpoints used to confirm third-party identifiers could cause excessive use of disk space and memory leading to resource exhaustion. Note that the groups feature is not part of the Matrix specification and the chosen maximum lengths are arbitrary. Not all clients might abide by them. Refer to referenced GitHub security advisory for additional details including workarounds.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24137	Directory traversal vulnerability in Wcms 0.3.2 allows an attacker to read arbitrary files on the server that is running an application via the path parameter to wex/cssjs.php.	5.3	More Details
CVE-2020-36315	In RELIC before 2020-08-01, RSA PKCS#1 v1.5 signature forgery can occur because certain checks of the padding (and of the first two bytes) are inadequate. NOTE: this requires that a low public exponent (such as 3) is being used. The product, by default, does not generate RSA keys with such a low number.	5.3	More Details
CVE-2021-1472	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	5.3	More Details
CVE-2021-1473	Multiple vulnerabilities exist in the web-based management interface of Cisco Small Business RV Series Routers. A remote attacker could execute arbitrary commands or bypass authentication and upload files on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24219	The Thrive Optimize WordPress plugin before 1.4.13.3, Thrive Comments WordPress plugin before 1.4.15.3, Thrive Headline Optimizer WordPress plugin before 1.3.7.3, Thrive Leads WordPress plugin before 2.3.9.4, Thrive Ultimatum WordPress plugin before 2.3.9.4, Thrive Quiz Builder WordPress plugin before 2.3.9.4, Thrive Apprentice WordPress plugin before 2.3.9.4, Thrive Visual Editor WordPress plugin before 2.6.7.4, Thrive Dashboard WordPress plugin before 2.3.9.3, Thrive Ovation WordPress plugin before 2.4.5, Thrive Clever Widgets WordPress plugin before 1.57.1 and Rise by Thrive Themes WordPress theme before 2.0.0, Ignition by Thrive Themes WordPress theme before 2.0.0, Luxe by Thrive Themes WordPress theme before 2.0.0, FocusBlog by Thrive Themes WordPress theme before 2.0.0, Minus by Thrive Themes WordPress theme before 2.0.0, Squared by Thrive Themes WordPress theme before 2.0.0, Voice WordPress theme before 2.0.0, Performag by Thrive Themes WordPress theme before 2.0.0, Pressive by Thrive Themes WordPress theme before 2.0.0, Storied by Thrive Themes WordPress theme before 2.0.0, Thrive Themes Builder WordPress theme before 2.2.4 register a REST API endpoint associated with Zapier functionality. While this endpoint was intended to require an API key in order to access, it was possible to access it by supplying an empty api_key parameter in vulnerable versions if Zapier was not enabled. Attackers could use this endpoint to add arbitrary data to a predefined option in the wp_options table.	5.3	More Details
CVE-2021-23368	The package postcss from 7.0.0 and before 8.2.10 are vulnerable to Regular Expression Denial of Service (ReDoS) during source map parsing.	5.3	More Details
CVE-2021-28876	In the standard library in Rust before 1.52.0, the Zip implementation has a panic safety issue. It calls __iterator_get_unchecked() more than once for the same index when the underlying iterator panics (in certain conditions). This bug could lead to a memory safety violation due to an unmet safety requirement for the TrustedRandomAccess trait.	5.3	More Details
CVE-2021-21728	A ZTE product has a configuration error vulnerability. Because a certain port is open by default, an attacker can consume system processing resources by flushing a large number of packets to the port, and successfully exploiting this vulnerability could reduce system processing capabilities. This affects: ZXA10 C300M all versions up to V4.3P8.	5.3	More Details
CVE-2021-27598	SAP NetWeaver AS JAVA (Customer Usage Provisioning Servlet), versions - 7.31, 7.40, 7.50, allows an attacker to read some statistical data like product version, traffic, timestamp etc. because of missing authorization check in the servlet.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29997	An issue was discovered in Wind River VxWorks 7 before 21.03. A specially crafted packet may lead to buffer over-read on IKE.	5.3	More Details
CVE-2020-36287	The dashboard gadgets preference resource of the Atlassian gadgets plugin used in Jira Server and Jira Data Center before version 8.13.5, and from version 8.14.0 before version 8.15.1 allows remote anonymous attackers to obtain gadget related settings via a missing permissions check.	5.3	More Details
CVE-2021-28450	Microsoft SharePoint Denial of Service Vulnerability	5.0	More Details
CVE-2021-21483	Under certain conditions SAP Solution Manager, version - 720, allows a high privileged attacker to get access to sensitive information which has a direct serious impact beyond the exploitable component thereby affecting the confidentiality in the application.	4.9	More Details
CVE-2021-28973	The XML Import functionality of the Administration console in Perforce Helix ALM 2020.3.1 Build 22 accepts XML input data that is parsed by insecurely configured software components, leading to XXE attacks.	4.9	More Details
CVE-2021-1406	A vulnerability in Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to improper inclusion of sensitive information in downloadable files. An attacker could exploit this vulnerability by authenticating to an affected device and issuing a specific set of commands. A successful exploit could allow the attacker to obtain hashed credentials of system users. To exploit this vulnerability an attacker would need to have valid user credentials with elevated privileges.	4.9	More Details
CVE-2021-29425	In Apache Commons IO before 2.7, When invoking the method FileNameUtils.normalize with an improper input string, like "//../foo", or "\\..\foo", the result would be the same value, thus possibly providing access to files in the parent directory, but not further above (thus "limited" path traversal), if the calling code would use the result to construct a path value.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0443	In several functions of ScreenshotHelper.java and related files, there is a possible incorrectly saved screenshot due to a race condition. This could lead to local information disclosure across user profiles with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-170474245	4.7	More Details
CVE-2021-1420	A vulnerability in certain web pages of Cisco Webex Meetings could allow an unauthenticated, remote attacker to modify a web page in the context of a user's browser. The vulnerability is due to improper checks on parameter values in affected pages. An attacker could exploit this vulnerability by persuading a user to follow a crafted link that is designed to pass HTML code into an affected parameter. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks.	4.7	More Details
CVE-2021-29438	The Nextcloud dialogs library (npm package @nextcloud/dialogs) before 3.1.2 insufficiently escaped text input passed to a toast. If your application displays toasts with user-supplied input, this could lead to a XSS vulnerability. The vulnerability has been patched in version 3.1.2 If you need to display HTML in the toast, explicitly pass the `options.isHTML` config flag.	4.6	More Details
CVE-2021-3473	An internal product security audit of Lenovo XClarity Controller (XCC) discovered that the XCC configuration backup/restore password may be written to an internal XCC log buffer if Lenovo XClarity Administrator (LXCA) is used to perform the backup/restore. The backup/restore password typically exists in this internal log buffer for less than 10 minutes before being overwritten. Generating an FFDC service log will include the log buffer contents, including the backup/restore password if present. The FFDC service log is only generated when requested by a privileged XCC user and it is only accessible to the privileged XCC user that requested the file. The backup/restore password is not captured if the backup/restore is initiated directly from XCC.	4.5	More Details
CVE-2021-23372	All versions of package mongo-express are vulnerable to Denial of Service (DoS) when exporting an empty collection as CSV, due to an unhandled exception, leading to a crash.	4.4	More Details
CVE-2021-27094	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28447	Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability	4.4	More Details
CVE-2021-30152	An issue was discovered in MediaWiki before 1.31.13 and 1.32.x through 1.35.x before 1.35.2. When using the MediaWiki API to "protect" a page, a user is currently able to protect to a higher level than they currently have permissions for.	4.3	More Details
CVE-2021-30155	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. ContentModelChange does not check if a user has correct permissions to create and set the content model of a nonexistent page.	4.3	More Details
CVE-2020-15942	An information disclosure vulnerability in Web Vulnerability Scan profile of Fortinet's FortiWeb version 6.2.x below 6.2.4 and version 6.3.x below 6.3.5 may allow a remote authenticated attacker to read the password used by the FortiWeb scanner to access the device defined in the scan profile.	4.3	More Details
CVE-2021-30159	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. Users can bypass intended restrictions on deleting pages in certain "fast double move" situations. MovePage::isValidMoveTarget() uses FOR UPDATE, but it's only called if Title::getArticleID() returns non-zero with no special flags. Next, MovePage::moveToInternal() will delete the page if getArticleID(READ_LATEST) is non-zero. Therefore, if the page is missing in the replica DB, isValidMove() will return true, and then moveToInternal() will unconditionally delete the page if it can be found in the master.	4.3	More Details
CVE-2021-27605	SAP's HCM Travel Management Fiori Apps V2, version - 608, does not perform proper authorization check, allowing an authenticated but unauthorized attacker to read personnel numbers of employees, resulting in escalation of privileges. However, the attacker can only read some information like last name, first name of the employees, so there is some loss of confidential information, Integrity and Availability are not impacted.	4.3	More Details
CVE-2021-1467	A vulnerability in Cisco Webex Meetings for Android could allow an authenticated, remote attacker to modify the avatar of another user. This vulnerability is due to improper authorization checks. An attacker could exploit this vulnerability by sending a crafted request to the Cisco Webex Meetings client of a targeted user of a meeting in which they are both participants. A successful exploit could allow the attacker to modify the avatar of the targeted user.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30156	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. Special:Contributions can leak that a "hidden" user exists.	4.3	More Details
CVE-2021-21639	Jenkins 2.286 and earlier, LTS 2.277.1 and earlier does not validate the type of object created after loading the data submitted to the `config.xml` REST API endpoint of a node, allowing attackers with Computer/Configure permission to replace a node with one of a different type.	4.3	More Details
CVE-2021-24024	A clear text storage of sensitive information into log file vulnerability in FortiADCManager 5.3.0 and below, 5.2.1 and below and FortiADC 5.3.7 and below may allow a remote authenticated attacker to read other local users' password in log files.	4.3	More Details
CVE-2021-21492	SAP NetWeaver Application Server Java(HTTP Service), versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not sufficiently validate logon group in URLs, resulting in a content spoofing vulnerability when directory listing is enabled.	4.3	More Details
CVE-2021-1399	A vulnerability in the Self Care Portal of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to modify data on an affected system without proper authorization. The vulnerability is due to insufficient validation of user-supplied data to the Self Care Portal. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could allow the attacker to modify information without proper authorization.	4.3	More Details
CVE-2013-1055	The unity-firefox-extension package could be tricked into dropping a C callback which was still in use, which Firefox would then free, causing Firefox to crash. This could be achieved by adding an action to the launcher and updating it with new callbacks until the libunity-webapps rate limit was hit. Fixed in 3.0.0+14.04.20140416-0ubuntu1.14.04.1 of unity-firefox-extension and in all versions of libunity-webapps by shipping an empty unity-firefox-extension package, thus disabling the extension entirely and invalidating the attack against the libunity-webapps package.	4.3	More Details
CVE-2013-1054	The unity-firefox-extension package could be tricked into destroying the Unity webapps context, causing Firefox to crash. This could be achieved by spinning the event loop inside the webapps initialization callback. Fixed in 3.0.0+14.04.20140416-0ubuntu1.14.04.1 by shipping an empty package, thus disabling the extension entirely.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4964	IBM Jazz Team Server products contain an undisclosed vulnerability that could allow an authenticated user to present a customized message on the application which could be used to phish other users. IBM X-Force ID: 192419.	4.3	More Details
CVE-2021-21641	A cross-site request forgery (CSRF) vulnerability in Jenkins promoted builds Plugin 3.9 and earlier allows attackers to to promote builds.	4.3	More Details
CVE-2021-21640	Jenkins 2.286 and earlier, LTS 2.277.1 and earlier does not properly check that a newly created view has an allowed name, allowing attackers with View/Create permission to create views with invalid or already-used names.	4.3	More Details
CVE-2021-28938	Siren Federate before 6.8.14-10.3.9, 6.9.x through 7.6.x before 7.6.2-20.2, 7.7.x through 7.9.x before 7.9.3-21.6, 7.10.x before 7.10.2-22.2, and 7.11.x before 7.11.2-23.0 can leak user information across thread contexts. This occurs in opportunistic circumstances when there is concurrent query execution by a low-privilege user and a high-privilege user. The former query might run with the latter query's privileges.	4.3	More Details
CVE-2021-25378	Improper access control of certain port in SmartThings prior to version 1.7.63.6 allows remote temporary denial of service.	4.3	More Details
CVE-2020-7924	Usage of specific command line parameter in MongoDB Tools which was originally intended to just skip hostname checks, may result in MongoDB skipping all certificate validation. This may result in accepting invalid certificates.This issue affects: MongoDB Inc. MongoDB Database Tools 3.6 versions later than 3.6.5; 3.6 versions prior to 3.6.21; 4.0 versions prior to 4.0.21; 4.2 versions prior to 4.2.11; 100 versions prior to 100.2.0. MongoDB Inc. Mongomirror 0 versions later than 0.6.0.	4.2	More Details
CVE-2021-3463	A null pointer dereference vulnerability in Lenovo Power Management Driver for Windows 10, prior to version 1.67.17.54, that could cause systems to experience a blue screen error.	4.2	More Details
CVE-2021-28316	Windows WLAN AutoConfig Service Security Feature Bypass Vulnerability	4.2	More Details
CVE-2021-25364	A pendingIntent hijacking vulnerability in Secure Folder prior to SMR APR-2021 Release 1 allows unprivileged applications to access contact information.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25359	An improper SELinux policy prior to SMR APR-2021 Release 1 allows local attackers to access AP information without proper permissions via untrusted applications.	4.0	More Details
CVE-2021-25379	Intent redirection vulnerability in Gallery prior to version 5.4.16.1 allows attacker to execute privileged action.	4.0	More Details
CVE-2021-29429	In Gradle before version 7.0, files created with open permissions in the system temporary directory can allow an attacker to access information downloaded by Gradle. Some builds could be vulnerable to a local information disclosure. Remote files accessed through TextResourceFactory are downloaded into the system temporary directory first. Sensitive information contained in these files can be exposed to other local users on the same system. If you do not use the `TextResourceFactory` API, you are not vulnerable. As of Gradle 7.0, uses of the system temporary directory have been moved to the Gradle User Home directory. By default, this directory is restricted to the user running the build. As a workaround, set a more restrictive umask that removes read access to other users. When files are created in the system temporary directory, they will not be accessible to other users. If you are unable to change your system's umask, you can move the Java temporary directory by setting the System Property `java.io.tmpdir`. The new path needs to limit permissions to the build user only.	4.0	More Details
CVE-2021-3448	A flaw was found in dnsmasq in versions before 2.85. When configured to use a specific server for a given network interface, dnsmasq uses a fixed port while forwarding queries. An attacker on the network, able to find the outgoing port used by dnsmasq, only needs to guess the random transmission ID to forge a reply and get it accepted by dnsmasq. This flaw makes a DNS Cache Poisoning attack much easier. The highest threat from this vulnerability is to data integrity.	4.0	More Details
CVE-2021-25358	A vulnerability that stores IMSI values in an improper path prior to SMR APR-2021 Release 1 allows local attackers to access IMSI values without any permission via untrusted applications.	4.0	More Details
CVE-2020-36314	fr-archive-libarchive.c in GNOME file-roller through 3.38.0, as used by GNOME Shell and other software, allows Directory Traversal during extraction because it lacks a check of whether a file's parent is a symlink in certain complex situations. NOTE: this issue exists because of an incomplete fix for CVE-2020-11736.	3.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22497	Advanced Authentication versions prior to 6.3 SP4 have a potential broken authentication due to improper session management issue.	3.8	More Details
CVE-2021-25377	Intent redirection in Samsung Experience Service versions 10.8.0.4 in Android P(9.0) below, and 12.2.0.5 in Android Q(10.0) above allows attacker to execute privileged action.	3.3	More Details
CVE-2021-28312	Windows NTFS Denial of Service Vulnerability	3.3	More Details
CVE-2021-29671	IBM Spectrum Scale 5.1.0.1 could allow a local attacker to bypass the filesystem audit logging mechanism when file audit logging is enabled. IBM X-Force ID: 199478.	3.3	More Details
CVE-2021-25376	An improper synchronization logic in Samsung Email prior to version 6.1.41.0 can leak messages in certain mailbox in plain text when STARTTLS negotiation is failed.	3.1	More Details
CVE-2020-8388	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8389	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8390	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8391	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8387	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8386	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8385	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8384	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8383	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8379	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8382	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8381	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8380	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8393	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8378	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8377	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8376	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8375	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8374	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8373	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8372	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8371	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8392	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8397	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8394	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8395	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2016-8181	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 2016. Notes: none	N/A	More Details
CVE-2021-3471	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-8180	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 2016. Notes: none	N/A	More Details
CVE-2016-8200	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 2016. Notes: none	N/A	More Details
CVE-2016-8197	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 2016. Notes: none	N/A	More Details
CVE-2020-8415	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8414	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8413	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8412	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8411	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8410	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8409	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8408	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8407	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8406	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8405	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8404	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8403	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8402	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8401	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8400	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8399	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8398	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8369	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8396	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8370	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8363	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8368	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2016-8190	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 2016. Notes: none	N/A	More Details
CVE-2016-8170	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 2016. Notes: none	N/A	More Details
CVE-2016-8198	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 2016. Notes: none	N/A	More Details
CVE-2016-8169	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 2016. Notes: none	N/A	More Details
CVE-2016-8168	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 2016. Notes: none	N/A	More Details
CVE-2021-3465	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-8167	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 2016. Notes: none	N/A	More Details
CVE-2016-8166	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 2016. Notes: none	N/A	More Details
CVE-2016-8165	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 2016. Notes: none	N/A	More Details
CVE-2016-8164	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 2016. Notes: none	N/A	More Details
CVE-2016-8163	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 2016. Notes: none	N/A	More Details
CVE-2016-8189	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 2016. Notes: none	N/A	More Details
CVE-2016-8162	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 2016. Notes: none	N/A	More Details
CVE-2016-8161	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 2016. Notes: none	N/A	More Details
CVE-2016-8188	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 2016. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-8187	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 2016. Notes: none	N/A	More Details
CVE-2016-8184	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 2016. Notes: none	N/A	More Details
CVE-2016-8186	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 2016. Notes: none	N/A	More Details
CVE-2016-8185	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 2016. Notes: none	N/A	More Details
CVE-2020-8626	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019	N/A	More Details
CVE-2020-8627	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019	N/A	More Details
CVE-2020-8628	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019	N/A	More Details
CVE-2020-8629	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019	N/A	More Details
CVE-2020-8630	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2019	N/A	More Details
CVE-2016-8171	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 2016. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-8172	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 2016. Notes: none	N/A	More Details
CVE-2020-8367	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2016-8173	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 2016. Notes: none	N/A	More Details
CVE-2020-8366	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8365	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8364	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8362	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8361	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8360	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8359	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-8358	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-8196	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 2016. Notes: none	N/A	More Details
CVE-2016-8179	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 2016. Notes: none	N/A	More Details
CVE-2016-8178	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 2016. Notes: none	N/A	More Details
CVE-2016-8195	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 2016. Notes: none	N/A	More Details
CVE-2016-8177	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 2016. Notes: none	N/A	More Details
CVE-2016-8176	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 2016. Notes: none	N/A	More Details
CVE-2016-8194	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 2016. Notes: none	N/A	More Details
CVE-2021-28421	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-21417. Reason: This candidate is a duplicate of CVE-2021-21417. Notes: All CVE users should reference CVE-2021-21417 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2016-8182	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 2016. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-8175	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 2016. Notes: none	N/A	More Details
CVE-2016-8183	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 2016. Notes: none	N/A	More Details
CVE-2016-8193	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 2016. Notes: none	N/A	More Details
CVE-2016-8174	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 2016. Notes: none	N/A	More Details
CVE-2016-8192	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 2016. Notes: none	N/A	More Details
CVE-2016-8191	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 2016. Notes: none	N/A	More Details
CVE-2016-8199	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 2016. Notes: none	N/A	More Details