SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 15 June 2022

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-2022-29226	Envoy is a cloud-native high-performance proxy. In versions prior to 1.22.1 the OAuth filter implementation does not include a mechanism for validating access tokens, so by design when the HMAC signed cookie is missing a full authentication flow should be triggered. However, the current implementation assumes that access tokens are always validated thus allowing access in the presence of any access token attached to the request. Users are advised to upgrade. There is no known workaround for this issue.	10.0	More Details
CVE-2022-25152	The ITarian platform (SAAS / on-premise) offers the possibility to run code on agents via a function called procedures. It is possible to require a mandatory approval process. Due to a vulnerability in the approval process, present in any version prior to 6.35.37347.20040, a malicious actor (with a valid session token) can create a procedure, bypass approval, and execute the procedure. This results in the ability for any user with a valid session token to perform arbitrary code execution and full system take-over on all agents.	9.9	More Details
CVE-2017-20039	A vulnerability was found in SICUNET Access Controller 0.32-05z. It has been classified as very critical. This affects an unknown part. The manipulation leads to weak authentication. It is possible to initiate the attack remotely.	9.8	More Details
CVE-2022-0885	The Member Hero WordPress plugin through 1.0.9 lacks authorization checks, and does not validate the a request parameter in an AJAX action, allowing unauthenticated users to call arbitrary PHP functions with no arguments.	9.8	More Details
CVE-2022-0827	The Bestbooks WordPress plugin through 2.6.3 does not sanitise and escape some parameters before using them in a SQL statement via an AJAX action, leading to an SQL Injection exploitable by unauthenticated users	9.8	More Details
CVE-2022-0786	The KiviCare WordPress plugin before 2.3.9 does not sanitise and escape some parameters before using them in SQL statements via the ajax_post AJAX action with the get_doctor_details route, leading to SQL Injections exploitable by unauthenticated users	9.8	More Details
CVE-2021-37404	There is a potential heap buffer overflow in Apache Hadoop libhdfs native code. Opening a file path provided by user without validation may result in a denial of service or arbitrary code execution. Users should upgrade to Apache Hadoop 2.10.2, 3.2.3, 3.3.2 or higher.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29525	Rakuten Casa version AP_F_V1_4_1 or AP_F_V2_0_0 uses a hard-coded credential which may allow a remote unauthenticated attacker to log in with the root privilege and perform an arbitrary operation.	9.8	More Details
CVE-2021-41749	In the SEOmatic plugin up to 3.4.11 for Craft CMS 3, it is possible for unauthenticated attackers to perform a Server-Side Template Injection, allowing for remote code execution.	9.8	More Details
CVE-2022-0788	The WP Fundraising Donation and Crowdfunding Platform WordPress plugin before 1.5.0 does not sanitise and escape a parameter before using it in a SQL statement via one of it's REST route, leading to an SQL injection exploitable by unauthenticated users	9.8	More Details
CVE-2022-31273	An issue in TopIDP3000 Topsec Operating System tos_3.3.005.665b.15_smpidp allows attackers to perform a brute-force attack via a crafted session_id cookie.	9.8	More Details
CVE-2021-41755	dynamicMarkt <= 3.10 is affected by SQL injection in the kat1 parameter of index.php.	9.8	More Details
CVE-2021-41754	dynamicMarkt <= 3.10 is affected by SQL injection in the parent parameter of index.php.	9.8	More Details
CVE-2022-31788	IdeaLMS 2022 allows SQL injection via the IdeaLMS/ChatRoom/ClassAccessControl/6?isBigBlueButton=0&ClassID= pathname.	9.8	More Details
CVE-2022-32563	An issue was discovered in Couchbase Sync Gateway 3.x before 3.0.2. Admin credentials are not verified when using X.509 client-certificate authentication from Sync Gateway to Couchbase Server. When Sync Gateway is configured to authenticate with Couchbase Server using X.509 client certificates, the admin credentials provided to the Admin REST API are ignored, resulting in privilege escalation for unauthenticated users. The Public REST API is not impacted by this issue. A workaround is to replace X.509 certificate based authentication with Username and Password authentication inside the bootstrap configuration.	9.8	More Details
CVE-2022-31813	Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.	9.8	More Details
CVE-2022-25651	Memory corruption in bluetooth host due to integer overflow while processing BT HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	9.8	More Details
CVE-2022-1768	The RSVPMaker plugin for WordPress is vulnerable to unauthenticated SQL Injection due to insufficient escaping and parameterization on user supplied data passed to multiple SQL queries in the ~/rsvpmaker-email.php file. This makes it possible for unauthenticated attackers to steal sensitive information from the database in versions up to, and including, 9.3.2. Please note that this is separate from CVE-2022-1453 & CVE-2022-1505.	9.8	More Details
CVE-2022-30308	In Festo Controller CECC-X-M1 product family in multiple versions, the http-endpoint "cecc-x-web-viewer-request-on" POST request doesn’t check for port syntax. This can result in unauthorized execution of system commands with root privileges due to improper access control command injection.	9.8	More Details
CVE-2022-30309	In Festo Controller CECC-X-M1 product family in multiple versions, the http-endpoint "cecc-x-web-viewer-request-off" POST request doesn’t check for port syntax. This can result in unauthorized execution of system commands with root privileges due to improper access control command injection.	9.8	More Details
CVE-2022-30310	In Festo Controller CECC-X-M1 product family in multiple versions, the http-endpoint "cecc-x-acknerr-request" POST request doesn’t check for port syntax. This can result in unauthorized execution of system commands with root privileges due to improper access control command injection.	9.8	More Details
CVE-2022-30311	In Festo Controller CECC-X-M1 product family in multiple versions, the http-endpoint "cecc-x-refresh-request" POST request doesn’t check for port syntax. This can result in unauthorized execution of system commands with root privileges due to improper access control command injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35104	Possible buffer overflow due to improper parsing of headers while playing the FLAC audio clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2021-40036	The bone voice ID TA has a memory overwrite vulnerability. Successful exploitation of this vulnerability may result in malicious code execution.	9.8	More Details
CVE-2022-33174	Power Distribution Units running on Powertek firmware (multiple brands) before 3.30.30 allows remote authorization bypass in the web interface. To exploit the vulnerability, an attacker must send an HTTP packet to the data retrieval interface (/cgi/get_param.cgi) with the tmpToken cookie set to an empty string followed by a semicolon. This bypasses an active session authorization check. This can be then used to fetch the values of protected sys.passwd and sys.su.name fields that contain the username and password in cleartext.	9.8	More Details
CVE-2022-33175	Power Distribution Units running on Powertek firmware (multiple brands) before 3.30.30 have an insecure permissions setting on the user.token field that is accessible to everyone through the /cgi/get_param.cgi HTTP API. This leads to disclosing active session ids of currently logged-in administrators. The session id can then be reused to act as the administrator, allowing reading of the cleartext password, or reconfiguring the device.	9.8	More Details
CVE-2022-29797	There is a buffer overflow vulnerability in CV81-WDM FW 01.70.49.29.46. Successful exploitation of this vulnerability may lead to privilege escalation.	9.8	More Details
CVE-2022-31053	Biscuit is an authentication and authorization token for microservices architectures. The Biscuit specification version 1 contains a vulnerable algorithm that allows malicious actors to forge valid Γ-signatures. Such an attack would allow an attacker to create a token with any access level. The version 2 of the specification mandates a different algorithm than gamma signatures and as such is not affected by this vulnerability. The Biscuit implementations in Rust, Haskell, Go, Java and Javascript all have published versions following the v2 specification. There are no known workarounds for this issue.	9.8	More Details
CVE-2021-41661	Church Management System version 1.0 is affected by a SQL anjection vulnerability through creating a user with a PHP file as an avatar image, which is accessible through the /uploads directory. This can lead to RCE on the web server by uploading a PHP webshell.	9.8	More Details
CVE-2021-41662	The South Gate Inn Online Reservation System v1.0 contains an SQL injection vulnerability that can be chained with a malicious PHP file upload, which is caused by improper file handling in the editImg function. This vulnerability leads to remote code execution.	9.8	More Details
CVE-2022-31446	Tenda AC18 router V15.03.05.19 and V15.03.05.05 was discovered to contain a remote code execution (RCE) vulnerability via the Mac parameter at ip/goform/WriteFacMac.	9.8	More Details
CVE-2022-25167	Apache Flume versions 1.4.0 through 1.9.0 are vulnerable to a remote code execution (RCE) attack when a configuration uses a JMS Source with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI to allow only the use of the java protocol or no protocol.	9.8	More Details
CVE-2021-30341	Improper buffer size validation of DSM packet received can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	9.8	More Details
CVE-2022-30230	A vulnerability has been identified in SICAM GridEdge Essential ARM (All versions < V2.6.6), SICAM GridEdge Essential Intel (All versions < V2.6.6), SICAM GridEdge Essential with GDS ARM (All versions < V2.6.6), SICAM GridEdge Essential with GDS Intel (All versions < V2.6.6). The affected software does not require authenticated access for privileged functions. This could allow an unauthenticated attacker to create a new user with administrative permissions.	9.8	More Details
CVE-2021-41756	dynamicMarkt <= 3.10 is affected by SQL injection in the kat parameter of index.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1986	OS Command Injection in GitHub repository gogs/gogs prior to 0.12.9.	9.8	More Details
CVE-2022-30915	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the UpdateSnat parameter at /goform/aspForm.	9.8	More Details
CVE-2022-30921	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the SetMobileAPInfoById parameter at /goform/aspForm.	9.8	More Details
CVE-2022-30920	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Edit_BasicSSID parameter at /goform/aspForm.	9.8	More Details
CVE-2022-30919	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Edit_BasicSSID_5G parameter at /goform/aspForm.	9.8	More Details
CVE-2022-30918	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Asp_SetTelnet parameter at /goform/aspForm.	9.8	More Details
CVE-2022-30917	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the AddWlanMacList parameter at /goform/aspForm.	9.8	More Details
CVE-2022-30916	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Asp_SetTelnetDebug parameter at /goform/aspForm.	9.8	More Details
CVE-2022-30914	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the UpdateMacClone parameter at /goform/aspForm.	9.8	More Details
CVE-2022-30924	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the SetAPWifiorLedInfoById parameter at /goform/aspForm.	9.8	More Details
CVE-2022-30913	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the ipqos_set_bandwidth parameter at /goform/aspForm.	9.8	More Details
CVE-2022-30912	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the UpdateWanParams parameter at /goform/aspForm.	9.8	More Details
CVE-2022-30910	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the GO parameter at /goform/aspForm.	9.8	More Details
CVE-2022-30909	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the CMD parameter at /goform/aspForm.	9.8	More Details
CVE-2022-32337	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/admin/patients/manage_patient.php?id=.	9.8	More Details
CVE-2022-1692	The CP Image Store with Slideshow WordPress plugin before 1.0.68 does not sanitise and escape the ordering_by query parameter before using it in a SQL statement in pages where the [codepeople-image-store] is embed, allowing unauthenticated users to perform an SQL injection attack	9.8	More Details
CVE-2022-30922	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the EditWlanMacList parameter at /goform/aspForm.	9.8	More Details
CVE-2022-30923	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the Asp_SetTimingtimeWifiAndLed parameter at /goform/aspForm.	9.8	More Details
CVE-2022-27668	Depending on the configuration of the route permission table in file 'saprouttab', it is possible for an unauthenticated attacker to execute SAProuter administration commands in SAP NetWeaver and ABAP Platform - versions KERNEL 7.49, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, KRNL64NUC 7.49, KRNL64UC 7.49, SAP_ROUTER 7.53, 7.22, from a remote client, for example stopping the SAProuter, that could highly impact systems availability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30925	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the AddMacList parameter at /goform/aspForm.	9.8	More Details
CVE-2022-31031	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In versions prior to and including 2.12.1 a stack buffer overflow vulnerability affects PJSIP users that use STUN in their applications, either by: setting a STUN server in their account/media config in PJSUA/PJSUA2 level, or directly using `pjlib-util/stun_simple` API. A patch is available in commit 450baca which should be included in the next release. There are no known workarounds for this issue.	9.8	More Details
CVE-2022-32272	OPSWAT MetaDefender Core before 5.1.2, MetaDefender ICAP before 4.12.1, and MetaDefender Email Gateway Security before 5.6.1 have incorrect access control, resulting in privilege escalation.	9.8	More Details
CVE-2022-31311	An issue in adm.cgi of WAVLINK AERIAL X 1200M M79X3.V5030.180719 allows attackers to execute arbitrary commands via a crafted POST request.	9.8	More Details
CVE-2022-32336	Fast Food Ordering System v1.0 is vulnerable to SQL Injection via /ffos/admin/menus/view_menu.php?id=.	9.8	More Details
CVE-2022-32352	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/classes/Master.php?f=delete_patient_admission.	9.8	More Details
CVE-2021-42675	Kreado Kreasfero 1.5 does not properly sanitize uploaded files to the media directory. One can upload a malicious PHP file and obtain remote code execution.	9.8	More Details
CVE-2021-35081	Possible buffer overflow due to improper validation of SSID length received from beacon or probe response during an IBSS session in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	9.8	More Details
CVE-2022-29013	A command injection in the command parameter of Razer Sila Gaming Router v2.0.441_api-2.0.418 allows attackers to execute arbitrary commands via a crafted POST request.	9.8	More Details
CVE-2022-31313	api-res-py package in PyPI 0.1 is vulnerable to a code execution backdoor in the request package.	9.8	More Details
CVE-2022-30882	pyanxdns package in PyPI version 0.2 is vulnerable to code execution backdoor. The impact is: execute arbitrary code (remote). When installing the pyanxdns package of version 0.2, the request package will be installed.	9.8	More Details
CVE-2022-30877	The keep for python, as distributed on PyPI, included a code-execution backdoor inserted by a third party. The current version, without this backdoor, is 1.2.	9.8	More Details
CVE-2021-40589	ZAngband zangband-data 2.7.5 is affected by an integer underflow vulnerability in src/tk/plat.c through the variable fileheader.bfOffBits.	9.8	More Details
CVE-2022-30926	H3C Magic R100 R100V100R005 was discovered to contain a stack overflow vulnerability via the EditMacList parameter at /goform/aspForm.	9.8	More Details
CVE-2021-35090	Possible hypervisor memory corruption due to TOC TOU race condition when updating address mappings in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	9.3	More Details
CVE-2022-32328	Fast Food Ordering System v1.0 is vulnerable to Delete any file. via /ffos/classes/Master.php?f=delete_img.	9.1	More Details
CVE-2021-35082	Improper integrity check can lead to race condition between tasks PDCP and RRC? right after a valid RRC security mode command packet has been received in Snapdragon Industrial IOT	9.1	More Details
CVE-2021-30347	Improper integrity check can lead to race condition between tasks PDCP and RRC? right after a valid RRC Command packet has been received in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32559	An issue was discovered in Couchbase Server before 7.0.4. Random HTTP requests lead to leaked metrics.	9.1	More Details
CVE-2021-30343	Improper integrity check can lead to race condition between tasks PDCP and RRC? after a valid RRC Command packet has been received in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	9.1	More Details
CVE-2021-30342	Improper integrity check can lead to race condition between tasks PDCP and RRC? after a valid RRC Command packet has been received in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	9.1	More Details
CVE-2021-40604	A Server-Side Request Forgery (SSRF) vulnerability in IPS Community Suite before 4.6.2 allows remote authenticated users to request arbitrary URLs or trigger deserialization via phar protocol when generating class names dynamically. In some cases an exploitation is possible by an unauthenticated user.	9.1	More Details
CVE-2022-31760	Dialog boxes can still be displayed even if the screen is locked in carrier-customized USSD services. Successful exploitation of this vulnerability may affect data integrity and confidentiality.	9.1	More Details
CVE-2022-2067	SQL Injection in GitHub repository francoisjacquet/rosariosis prior to 9.0.	9.1	More Details
CVE-2022-28615	Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.	9.1	More Details
CVE-2022-1992	Path Traversal in GitHub repository gogs/gogs prior to 0.12.9.	9.1	More Details
CVE-2022-31830	Kity Minder v1.3.5 was discovered to contain a Server-Side Request Forgery (SSRF) via the init function at ImageCapture.class.php.	9.1	More Details
CVE-2022-31827	MonstaFTP v2.10.3 was discovered to contain a Server-Side Request Forgery (SSRF) via the function performFetchRequest at HTTPFetcher.php.	9.1	More Details
CVE-2022-31393	Jizhicms v2.2.5 was discovered to contain a Server-Side Request Forgery (SSRF) vulnerability via the Index function in app/admin/c/PluginsController.php.	9.1	More Details
CVE-2022-31390	Jizhicms v2.2.5 was discovered to contain a Server-Side Request Forgery (SSRF) vulnerability via the Update function in app/admin/c/TemplateController.php.	9.1	More Details
CVE-2022-31386	A Server-Side Request Forgery (SSRF) in the getFileBinary function of nbnbk cms 3 allows attackers to force the application to make arbitrary requests via injection of arbitrary URLs into the URL parameter.	9.1	More Details
CVE-2022-24840	django-s3file is a lightweight file upload input for Django and Amazon S3 . In versions prior to 5.5.1 it was possible to traverse the entire AWS S3 bucket and in most cases to access or delete files. If the `AWS_LOCATION` setting was set, traversal was limited to that location only. The issue was discovered by the maintainer. There were no reports of the vulnerability being known to or exploited by a third party, prior to the release of the patch. The vulnerability has been fixed in version 5.5.1 and above. There is no feasible workaround. We must urge all users to immediately updated to a patched version.	9.1	More Details
CVE-2022-1996	Authorization Bypass Through User-Controlled Key in GitHub repository emicklei/go-restful prior to v3.8.0.	9.1	More Details
CVE-2021-30339	Reading PRNG output may lead to improper key generation due to lack of buffer validation in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21122	The package metacalc before 0.0.2 are vulnerable to Arbitrary Code Execution when it exposes JavaScript's Math class to the v8 context. As the Math class is exposed to user-land, it can be used to get access to JavaScript's Function constructor.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-32278	XFCE 4.16 allows attackers to execute arbitrary code because xdg-open can execute a .desktop file on an attacker-controlled FTP server.	8.8	More Details
CVE-2022-25806	An issue was discovered in the IGEL Universal Management Suite (UMS) 6.07.100. A hardcoded DES key in the PrefDBCredentials class allows an attacker, who has discovered encrypted superuser credentials, to decrypt those credentials using a static 8-byte DES key.	8.8	More Details
CVE-2022-22479	IBM Spectrum Copy Data Management 2.2.0.0through 2.2.15.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 225887.	8.8	More Details
CVE-2021-40961	CMS Made Simple <=2.2.15 is affected by SQL injection in modules/News/function.admin_articlestab.php. The $sortby variable is concatenated with $query1, but it is possible to inject arbitrary SQL language without using the '.	8.8	More Details
CVE-2022-32562	An issue was discovered in Couchbase Server before 7.0.4. Operations may succeed on a collection using stale RBAC permission.	8.8	More Details
CVE-2022-30075	In TP-Link Router AX50 firmware 210730 and older, import of a malicious backup file via web interface can lead to remote code execution due to improper validation.	8.8	More Details
CVE-2022-1969	The Mobile browser color select plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.1. This is due to missing or incorrect nonce validation on the admin_update_data() function. This makes it possible for unauthenticated attackers to inject malicious web scripts via forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2022-1749	The WPMK Ajax Finder WordPress plugin is vulnerable to Cross-Site Request Forgery via the createplugin_atf_admin_setting_page() function found in the ~/inc/config/create-plugin-config.php file due to a missing nonce check which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.1.	8.8	More Details
CVE-2022-1657	Vulnerable versions of the Jupiter (<= 6.10.1) and JupiterX (<= 2.0.6) Themes allow logged-in users, including subscriber-level users, to perform Path Traversal and Local File inclusion. In the JupiterX theme, the jupiterx_cp_load_pane_action AJAX action present in the lib/admin/control-panel/control-panel.php file calls the load_control_panel_pane function. It is possible to use this action to include any local PHP file via the slug parameter. The Jupiter theme has a nearly identical vulnerability which can be exploited via the mka_cp_load_pane_action AJAX action present in the framework/admin/control-panel/logic/functions.php file, which calls the mka_cp_load_pane_action function.	8.8	More Details
CVE-2022-1654	Jupiter Theme <= 6.10.1 and JupiterX Core Plugin <= 2.0.7 allow any authenticated attacker, including a subscriber or customer-level attacker, to gain administrative privileges via the "abb_uninstall_template" (both) and "jupiterx_core_cp_uninstall_template" (JupiterX Core Only) AJAX actions	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1918	The ToolBar to Share plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.0. This is due to missing nonce validation on the plugin_toolbar_comparte page. This makes it possible for unauthenticated attackers to update the plugins settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2022-1900	The Copify plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.3.0. This is due to missing nonce validation on the CopifySettings page. This makes it possible for unauthenticated attackers to update the plugins settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2022-31496	LibreHealth EHR Base 2.0.0 allows incorrect interface/super/manage_site_files.php access.	8.8	More Details
CVE-2022-1777	The Filr WordPress plugin before 1.2.2.1 does not have authorisation check in two of its AJAX actions, allowing them to be called by any authenticated users, such as subscriber. They are are protected with a nonce, however the nonce is leaked on the dashboard. This could allow them to upload arbitrary HTML files as well as delete all files or arbitrary ones.	8.8	More Details
CVE-2022-1765	The Hot Linked Image Cacher WordPress plugin through 1.16 is vulnerable to CSRF. This can be used to store / cache images from external domains on the server, which could lead to legal risks (due to copyright violations or licensing rules).	8.8	More Details
CVE-2022-1758	The Genki Pre-Publish Reminder WordPress plugin through 1.4.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and lead to Stored XSS as well as RCE when custom code is added via the plugin settings.	8.8	More Details
CVE-2021-36710	ToaruOS 1.99.2 is affected by incorrect access control via the kernel. Improper MMU management and having a low GDT address allows it to be mapped in userland. A call gate can then be written to escalate to CPL 0.	8.8	More Details
CVE-2022-2064	Insufficient Session Expiration in GitHub repository nocodb/nocodb prior to 0.91.7+.	8.8	More Details
CVE-2022-2063	Improper Privilege Management in GitHub repository nocodb/nocodb prior to 0.91.7+.	8.8	More Details
CVE-2021-41738	ZeroShell 3.9.5 has a command injection vulnerability in /cgi-bin/kerbynet IP parameter, which may allow an authenticated attacker to execute system commands.	8.8	More Details
CVE-2021-44117	A Cross Site Request Forgery (CSRF) vulnerability exists in TheDayLightStudio Fuel CMS 1.5.0 via a POST call to /fuel/sitevariables/delete/4.	8.8	More Details
CVE-2022-1683	The amtyThumb WordPress plugin through 4.2.0 does not sanitise and escape a parameter before using it in a SQL statement via its shortcode, leading to an SQL injection and is exploitable by any authenticated user (and not just Author+ like the original advisory mention) due to the fact that they can execute shortcodes via an AJAX action	8.8	More Details
CVE-2021-44582	A Privilege Escalation vulnerability exists in Sourcecodester Money Transfer Management System 1.0, which allows a remote malicious user to gain elevated privileges to the Admin role via any URL.	8.8	More Details
CVE-2022-31595	SAP Financial Consolidation - version 1010,&#65533;does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40633	A memory leak (out-of-memory) in gif2rgb in util/gif2rgb.c in giflib 5.1.4 allows remote attackers trigger an out of memory exception or denial of service via a gif format file.	8.8	More Details
CVE-2021-35123	Buffer copy in GATT multi notification due to improper length check for the data coming over-the-air in Snapdragon Connectivity, Snapdragon Industrial IOT	8.8	More Details
CVE-2022-32262	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.1). The affected application contains a file upload server that is vulnerable to command injection. An attacker could use this to achieve arbitrary code execution.	8.8	More Details
CVE-2022-1703	Improper neutralization of special elements in the SonicWall SSL-VPN SMA100 series management interface allows a remote authenticated attacker to inject OS Commands which potentially leads to remote command execution vulnerability or denial of service (DoS) attack.	8.8	More Details
CVE-2022-32251	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.1). There is a missing authentication verification for a resource used to change the roles and permissions of a user. This could allow an attacker to change the permissions of any user and gain the privileges of an administrative user.	8.8	More Details
CVE-2022-31619	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.13), Teamcenter V13.0 (All versions < V13.0.0.9), Teamcenter V13.1 (All versions < V13.1.0.9), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.3), Teamcenter V14.0 (All versions < V14.0.0.2). Java EE Server Manager HTML Adaptor in Teamcenter consists of default hardcoded credentials. Access to the application allows a user to perform a series of actions that could potentially lead to remote code execution with elevated permissions.	8.8	More Details
CVE-2022-26476	A vulnerability has been identified in Spectrum Power 4 (All versions using Shared HIS), Spectrum Power 7 (All versions using Shared HIS), Spectrum Power MGMS (All versions using Shared HIS). An unauthenticated attacker could log into the component Shared HIS used in Spectrum Power systems by using an account with default credentials. A successful exploitation could allow the attacker to access the component Shared HIS with administrative privileges.	8.8	More Details
CVE-2021-35091	Possible out of bounds read due to improper typecasting while handling page fault for global memory in Snapdragon Connectivity, Snapdragon Mobile	8.4	More Details
CVE-2022-22085	Memory corruption in video due to buffer overflow while reading the dts file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-41641	Deno <=1.14.0 file sandbox does not handle symbolic links correctly. When running Deno with specific write access, the Deno.symlink method can be used to gain access to any directory.	8.4	More Details
CVE-2022-2054	Code Injection in GitHub repository nuitka/nuitka prior to 0.9.	8.4	More Details
CVE-2022-22090	Memory corruption in audio due to use after free while managing buffers from internal cache in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile	8.4	More Details
CVE-2022-22084	Memory corruption when extracting qcp audio file due to lack of check on data length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-35095	Improper serialization of message queue client registration can lead to race condition allowing multiple gunyah message clients to register with same label in Snapdragon Connectivity, Snapdragon Mobile	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22082	Memory corruption due to possible buffer overflow while parsing DSF header with corrupted channel count in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2022-22071	Possible use after free when process shell memory is freed using IOCTL munmap call and process initialization is in progress in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	8.4	More Details
CVE-2022-22068	kernel event may contain unexpected content which is not generated by NPU software in asynchronous execution mode in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2022-22057	Use after free in graphics fence due to a race condition while closing fence file descriptor and destroy graphics timeline simultaneously in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	8.4	More Details
CVE-2021-35130	Memory corruption in graphics support layer due to use after free condition in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	8.4	More Details
CVE-2021-35126	Memory corruption in DSP service due to improper validation of input parameters in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details
CVE-2021-30281	Possible unauthorized access to secure space due to improper check of data allowed while flashing the no access control device configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	8.4	More Details
CVE-2021-30334	Possible use after free due to lack of null check of DRM file status after file structure is freed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-35114	Improper buffer initialization on the backend driver can lead to buffer overflow in Snapdragon Auto	8.4	More Details
CVE-2021-35112	A user with user level permission can access graphics protected region due to improper access control in register configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-30350	Lack of MBN header size verification against input buffer can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	8.4	More Details
CVE-2022-29095	Dell SupportAssist Client Consumer versions (3.10.4 and prior) and Dell SupportAssist Client Commercial versions (3.1.1 and prior) contain a cross-site scripting vulnerability. A remote unauthenticated malicious user could potentially exploit this vulnerability under specific conditions leading to execution of malicious code on a vulnerable system.	8.3	More Details
CVE-2022-29255	Vyper is a Pythonic Smart Contract Language for the ethereum virtual machine. In versions prior to 0.3.4 when a calling an external contract with no return value, the contract address (including side effects) could be evaluated twice. This may result in incorrect outcomes for contracts. This issue has been addressed in v0.3.4.	8.2	More Details
CVE-2021-30349	Improper access control sequence for AC database after memory allocation can lead to possible memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35083	Possible out of bound read due to improper validation of certificate chain in SSL or Internet key exchange in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.2	More Details
CVE-2022-25845	The package com.alibaba:fastjson before 1.2.83 are vulnerable to Deserialization of Untrusted Data by bypassing the default autoType shutdown restrictions, which is possible under certain conditions. Exploiting this vulnerability allows attacking remote servers. Workaround: If upgrading is not possible, you can enable [safeMode](https://github.com/alibaba/fastjson/wiki/fastjson_safemode).	8.1	More Details
CVE-2022-25863	The package gatsby-plugin-mdx before 2.14.1, from 3.0.0 and before 3.15.2 are vulnerable to Deserialization of Untrusted Data when passing input through to the gray-matter package, due to its default configurations that are missing input sanitization. Exploiting this vulnerability is possible when passing input in both webpack (MDX files in src/pages or MDX file imported as a component in frontend / React code) and data mode (querying MDX nodes via GraphQL). Workaround: If an older version of gatsby-plugin-mdx must be used, input passed into the plugin should be sanitized ahead of processing.	8.1	More Details
CVE-2022-29250	GLPI is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. In versions prior to version 10.0.1 it is possible to add extra information by SQL injection on search pages. In order to exploit this vulnerability a user must be logged in.	8.1	More Details
CVE-2022-1993	Path Traversal in GitHub repository gogs/gogs prior to 0.12.9.	8.1	More Details
CVE-2022-1791	The One Click Plugin Updater WordPress plugin through 2.4.14 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and disable / hide the badge of the available updates and the related check.	8.1	More Details
CVE-2021-40668	The Android application HTTP File Server (Version 1.4.1) by 'slowscript' is affected by a path traversal vulnerability that permits arbitrary directory listing, file read, and file write.	8.1	More Details
CVE-2022-24065	The package cookiecutter before 2.1.1 are vulnerable to Command Injection via hg argument injection. When calling the cookiecutter function from Python code with the checkout parameter, it is passed to the hg checkout command in a way that additional flags can be set. The additional flags can be used to perform a command injection.	8.1	More Details
CVE-2022-1779	The Auto Delete Posts WordPress plugin through 1.3.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and delete specific posts, categories and attachments at once.	8.1	More Details
CVE-2022-2037	Excessive Attack Surface in GitHub repository tooljet/tooljet prior to v1.16.0.	8.0	More Details
CVE-2022-2027	Improper Neutralization of Formula Elements in a CSV File in GitHub repository kromitgmbh/titra prior to 0.77.0.	8.0	More Details
CVE-2022-27176	Incomplete filtering of special elements vulnerability exists in RevoWorks SCVX using 'File Sanitization Library' 1.043 and prior versions, RevoWorks Browser 2.2.67 and prior versions (when using 'File Sanitization Option'), and RevoWorks Desktop 2.1.84 and prior versions (when using 'File Sanitization Option'), which may allow an attacker to execute a malicious macro by having a user to download, import, and open a specially crafted file in the local environment.	7.8	More Details
CVE-2022-25153	The ITarian Endpoint Manage Communication Client, prior to version 6.43.41148.21120, is compiled using insecure OpenSSL settings. Due to this setting, a malicious actor with low privileges access to a system can escalate his privileges to SYSTEM abusing an insecure openssl.conf lookup.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31214	A Privilege Context Switching issue was discovered in join.c in Firejail 0.9.68. By crafting a bogus Firejail container that is accepted by the Firejail setuid-root program as a join target, a local attacker can enter an environment in which the Linux user namespace is still the initial user namespace, the NO_NEW_PRIVS prctl is not activated, and the entered mount namespace is under the attacker's control. In this way, the filesystem layout can be adjusted to gain root privileges through execution of available setuid-root binaries such as su or sudo.	7.8	More Details
CVE-2021-46818	Adobe Media Encoder version 15.4 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious M4A file.	7.8	More Details
CVE-2021-35102	Possible buffer overflow due to lack of validation for the length of NAI string read from EFS in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile	7.8	More Details
CVE-2021-35094	Improper verification of timeout-based authentication in identity credential can lead to invalid authorization in HLOS in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	7.8	More Details
CVE-2022-30790	Das U-Boot 2022.01 has a Buffer Overflow, a different issue than CVE-2022-30552.	7.8	More Details
CVE-2022-24077	Naver Cloud Explorer Beta allows the attacker to execute arbitrary code as System privilege via malicious DLL injection.	7.8	More Details
CVE-2021-35072	Possible buffer overflow due to improper validation of array index while processing external DIAG command in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details
CVE-2022-31762	The AMS module has a vulnerability in input validation. Successful exploitation of this vulnerability may cause privilege escalation.	7.8	More Details
CVE-2022-30703	Trend Micro Security 2021 and 2022 (Consumer) is vulnerable to an exposed dangerous method vulnerability that could allow an attacker to obtain access to leaked kernel addresses and disclose sensitive information. This vulnerability could also potentially be chained for privilege escalation.	7.8	More Details
CVE-2021-46817	Adobe Media Encoder version 15.4 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious M4A file.	7.8	More Details
CVE-2022-29925	Access of uninitialized pointer vulnerability exists in the simulator module contained in the graphic editor 'V-SFT' versions prior to v6.1.6.0, which may allow an attacker to obtain information and/or execute arbitrary code by having a user to open a specially crafted image file.	7.8	More Details
CVE-2022-29524	Out-of-bounds write vulnerability exists in V-Server v4.0.11.0 and earlier and V-Server Lite v4.0.13.0 and earlier, which may allow an attacker to obtain information and/or execute arbitrary code by having a user to open a specially crafted image file.	7.8	More Details
CVE-2022-29522	Use after free vulnerability exists in the simulator module contained in the graphic editor 'V-SFT' versions prior to v6.1.6.0, which may allow an attacker to obtain information and/or execute arbitrary code by having a user to open a specially crafted image file.	7.8	More Details
CVE-2022-29506	Out-of-bounds read vulnerability exist in the simulator module contained in the graphic editor 'V-SFT' v6.1.3.0 and earlier, which may allow an attacker to obtain information and/or execute arbitrary code by having a user to open a specially crafted image file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27502	RealVNC VNC Server 6.9.0 through 5.1.0 for Windows allows local privilege escalation because an installer repair operation executes %TEMP% files as SYSTEM.	7.8	More Details
CVE-2022-26302	Heap-based buffer overflow exists in the simulator module contained in the graphic editor 'V-SFT' versions prior to v6.1.6.0, which may allow an attacker to obtain information and/or execute arbitrary code by having a user to open a specially crafted image file.	7.8	More Details
CVE-2021-35129	Memory corruption in BT controller due to improper length check while processing vendor specific commands in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.8	More Details
CVE-2022-1202	The WP-CRM WordPress plugin through 1.2.1 does not validate and sanitise fields when exporting people to a CSV file, leading to a CSV injection vulnerability.	7.8	More Details
CVE-2021-46816	Adobe Premiere Pro version 15.4 (and earlier) are affected by a memory corruption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious M4A file.	7.8	More Details
CVE-2022-2042	Use After Free in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-32981	An issue was discovered in the Linux kernel through 5.18.3 on powerpc 32-bit platforms. There is a buffer overflow in ptrace PEEKUSER and POKEUSER (aka PEEKUSR and POKEUSR) when accessing floating point registers.	7.8	More Details
CVE-2022-1998	A use after free in the Linux kernel File System notify functionality was found in the way user triggers copy_info_records_to_user() call to fail in copy_event_to_user(). A local user could use this flaw to crash the system or potentially escalate their privileges on the system.	7.8	More Details
CVE-2022-31465	A vulnerability has been identified in Xpedition Designer VX.2.10 (All versions < VX.2.10 Update 13), Xpedition Designer VX.2.11 (All versions < VX.2.11 Update 11), Xpedition Designer VX.2.12 (All versions < VX.2.12 Update 5), Xpedition Designer VX.2.13 (All versions < VX.2.13 Update 1). The affected application assigns improper access rights to the service executable. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges.	7.8	More Details
CVE-2022-31590	SAP PowerDesigner Proxy - version 16.7, allows an attacker with low privileges and has local access, with the ability to work around system's root disk access restrictions to Write/Create a program file on system disk root path, which could then be executed with elevated privileges of the application during application start up or reboot, potentially compromising Confidentiality, Integrity and Availability of the system.	7.8	More Details
CVE-2022-22103	Memory corruption in multimedia driver due to double free while processing data from user in Snapdragon Auto	7.8	More Details
CVE-2022-2000	Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-22072	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	7.8	More Details
CVE-2022-29092	Dell SupportAssist Client Consumer versions (3.11.0 and versions prior) and Dell SupportAssist Client Commercial versions (3.2.0 and versions prior) contain a privilege escalation vulnerability. A non-admin user can exploit the vulnerability and gain admin access to the system.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35116	APK can load a crafted model into the CDSP which can lead to a compromise of CDSP and other APK`s data executing there in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	7.7	More Details
CVE-2022-31041	Open Forms is an application for creating and publishing smart forms. Open Forms supports file uploads as one of the form field types. These fields can be configured to allow only certain file extensions to be uploaded by end users (e.g. only PDF / Excel / ...). The input validation of uploaded files is insufficient in versions prior to 1.0.9 and 1.1.1. Users could alter or strip file extensions to bypass this validation. This results in files being uploaded to the server that are of a different file type than indicated by the file name extension. These files may be downloaded (manually or automatically) by staff and/or other applications for further processing. Malicious files can therefore find their way into internal/trusted networks. Versions 1.0.9 and 1.1.1 contain patches for this issue. As a workaround, an API gateway or intrusion detection solution in front of open-forms may be able to scan for and block malicious content before it reaches the Open Forms application.	7.6	More Details
CVE-2022-31753	The voice wakeup module has a vulnerability of using externally-controlled format strings. Successful exploitation of this vulnerability may affect system availability.	7.5	More Details
CVE-2022-31055	kCTF is a Kubernetes-based infrastructure for capture the flag (CTF) competitions. Prior to version 1.6.0, the kctf cluster set-src-ip-ranges was broken and allowed traffic from any IP. The problem has been patched in v1.6.0. As a workaround, those who want to test challenges privately can mark them as `public: false` and use `kctf chal debug port-forward` to connect.	7.5	More Details
CVE-2021-46813	Vulnerability of residual files not being deleted after an update in the ChinaDRM module. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2021-46812	The Device Manager has a vulnerability in multi-device interaction. Successful exploitation of this vulnerability may affect data integrity.	7.5	More Details
CVE-2022-31754	Logical defects in code implementation in some products. Successful exploitation of this vulnerability may affect the availability of some features.	7.5	More Details
CVE-2022-24278	The package convert-svg-core before 0.6.4 are vulnerable to Directory Traversal due to improper sanitization of SVG tags. Exploiting this vulnerability is possible by using a specially crafted SVG file.	7.5	More Details
CVE-2022-24429	The package convert-svg-core before 0.6.3 are vulnerable to Arbitrary Code Injection when using a specially crafted SVG file. An attacker can read arbitrary files from the file system and then show the file content as a converted PNG file.	7.5	More Details
CVE-2022-25851	The package jpeg-js before 0.4.4 are vulnerable to Denial of Service (DoS) where a particular piece of input will cause to enter an infinite loop and never return.	7.5	More Details
CVE-2022-31757	The setting module has a vulnerability of improper use of APIs. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2021-46814	The video framework has an out-of-bounds memory read/write vulnerability. Successful exploitation of this vulnerability may affect system availability.	7.5	More Details
CVE-2022-30780	Lighttpd 1.4.56 through 1.4.58 allows a remote attacker to cause a denial of service (CPU consumption from stuck connections) because connection_read_header_more in connections.c has a typo that disrupts use of multiple read operations on large headers.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2013	In Octopus Server after version 2022.1.1495 and before 2022.1.2647 if private spaces were enabled via the experimental feature flag all new users would have access to the Script Console within their private space.	7.5	More Details
CVE-2022-26834	Improper access control vulnerability in Rakuten Casa version AP_F_V1_4_1 or AP_F_V2_0_0 allows a remote attacker to obtain the information stored in the product because the product is set to accept HTTP connections from the WAN side by default.	7.5	More Details
CVE-2022-2062	Generation of Error Message Containing Sensitive Information in GitHub repository nocodb/nocodb prior to 0.91.7+.	7.5	More Details
CVE-2022-1762	The iQ Block Country WordPress plugin before 1.2.20 does not properly checks HTTP headers in order to validate the origin IP address, allowing threat actors to bypass it's block feature by spoofing the headers.	7.5	More Details
CVE-2020-14125	A denial of service vulnerability exists in some Xiaomi models of phones. The vulnerability is caused by out-of-bound read/write and can be exploited by attackers to make denial of service.	7.5	More Details
CVE-2022-28382	An issue was discovered in certain Verbatim drives through 2022-03-31. Due to the use of an insecure encryption AES mode (Electronic Codebook, aka ECB), an attacker may be able to extract information even from encrypted data, for example by observing repeating byte patterns. The firmware of the USB-to-SATA bridge controller INIC-3637EN uses AES-256 with the ECB mode. This operation mode of block ciphers (e.g., AES) always encrypts identical plaintext data, in this case blocks of 16 bytes, to identical ciphertext data. For some data, for instance bitmap images, the lack of the cryptographic property called diffusion, within ECB, can leak sensitive information even in encrypted data. Thus, the use of the ECB operation mode can put the confidentiality of specific information at risk, even in an encrypted form. This affects Keypad Secure USB 3.2 Gen 1 Drive Part Number #49428, Store 'n' Go Secure Portable HDD GD25LK01-3637-C VER4.0, Executive Fingerprint Secure SSD GDMSFE01-INI3637-C VER1.1, and Fingerprint Secure Portable Hard Drive Part Number #53650.	7.5	More Details
CVE-2022-1412	The Log WP_Mail WordPress plugin through 0.1 saves sent email in a publicly accessible directory using predictable filenames, allowing any unauthenticated visitor to obtain potentially sensitive information like generated passwords.	7.5	More Details
CVE-2022-29798	There is a denial of service vulnerability in CV81-WDM FW versions 01.70.49.29.46. Successful exploitation could cause denial of service.	7.5	More Details
CVE-2022-24296	Use of a Broken or Risky Cryptographic Algorithm vulnerability in Air Conditioning System G-150AD Ver. 3.21 and prior, Air Conditioning System AG-150A-A Ver. 3.21 and prior, Air Conditioning System AG-150A-J Ver. 3.21 and prior, Air Conditioning System GB-50AD Ver. 3.21 and prior, Air Conditioning System GB-50ADA-A Ver. 3.21 and prior, Air Conditioning System GB-50ADA-J Ver. 3.21 and prior, Air Conditioning System EB-50GU-A Ver. 7.10 and prior, Air Conditioning System EB-50GU-J Ver. 7.10 and prior, Air Conditioning System AE-200J Ver. 7.97 and prior, Air Conditioning System AE-200A Ver. 7.97 and prior, Air Conditioning System AE-200E Ver. 7.97 and prior, Air Conditioning System AE-50J Ver. 7.97 and prior, Air Conditioning System AE-50A Ver. 7.97 and prior, Air Conditioning System AE-50E Ver. 7.97 and prior, Air Conditioning System EW-50J Ver. 7.97 and prior, Air Conditioning System EW-50A Ver. 7.97 and prior, Air Conditioning System EW-50E Ver. 7.97 and prior, Air Conditioning System TE-200A Ver. 7.97 and prior, Air Conditioning System TE-50A Ver. 7.97 and prior and Air Conditioning System TW-50A Ver. 7.97 and prior allows a remote unauthenticated attacker to cause a disclosure of encrypted message of the air conditioning systems by sniffing encrypted communications.	7.5	More Details
CVE-2022-31761	Configuration defects in the secure OS module. Successful exploitation of this vulnerability will affect confidentiality.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31649	ownCloud owncloud/core before 10.10.0 Improperly Removes Sensitive Information Before Storage or Transfer.	7.5	More Details
CVE-2022-31054	Argo Events is an event-driven workflow automation framework for Kubernetes. Prior to version 1.7.1, several `HandleRoute` endpoints make use of the deprecated `ioutil.ReadAll()`. `ioutil.ReadAll()` reads all the data into memory. As such, an attacker who sends a large request to the Argo Events server will be able to crash it and cause denial of service. A patch for this vulnerability has been released in Argo Events version 1.7.1.	7.5	More Details
CVE-2021-40660	An issue was discovered in Delight Nashorn Sandbox 0.2.0. There is an ReDoS vulnerability that can be exploited to launching a denial of service (DoS) attack.	7.5	More Details
CVE-2021-37182	A vulnerability has been identified in SCALANCE XM408-4C (All versions < V6.5), SCALANCE XM408-4C (L3 int.) (All versions < V6.5), SCALANCE XM408-8C (All versions < V6.5), SCALANCE XM408-8C (L3 int.) (All versions < V6.5), SCALANCE XM416-4C (All versions < V6.5), SCALANCE XM416-4C (L3 int.) (All versions < V6.5), SCALANCE XR524-8C, 1x230V (All versions < V6.5), SCALANCE XR524-8C, 1x230V (L3 int.) (All versions < V6.5), SCALANCE XR524-8C, 24V (All versions < V6.5), SCALANCE XR524-8C, 24V (L3 int.) (All versions < V6.5), SCALANCE XR524-8C, 2x230V (All versions < V6.5), SCALANCE XR524-8C, 2x230V (L3 int.) (All versions < V6.5), SCALANCE XR526-8C, 1x230V (All versions < V6.5), SCALANCE XR526-8C, 1x230V (L3 int.) (All versions < V6.5), SCALANCE XR526-8C, 24V (All versions < V6.5), SCALANCE XR526-8C, 24V (L3 int.) (All versions < V6.5), SCALANCE XR526-8C, 2x230V (All versions < V6.5), SCALANCE XR526-8C, 2x230V (L3 int.) (All versions < V6.5), SCALANCE XR528-6M (All versions < V6.5), SCALANCE XR528-6M (2HR2) (All versions < V6.5), SCALANCE XR528-6M (2HR2, L3 int.) (All versions < V6.5), SCALANCE XR528-6M (L3 int.) (All versions < V6.5), SCALANCE XR552-12M (All versions < V6.5), SCALANCE XR552-12M (2HR2) (All versions < V6.5), SCALANCE XR552-12M (2HR2) (All versions < V6.5), SCALANCE XR552-12M (2HR2, L3 int.) (All versions < V6.5). The OSPF protocol implementation in affected devices fails to verify the checksum and length fields in the OSPF LS Update messages. An unauthenticated remote attacker could exploit this vulnerability to cause interruptions in the network by sending specially crafted OSPF packets. Successful exploitation requires OSPF to be enabled on an affected device.	7.5	More Details
CVE-2022-22064	Possible buffer over read due to lack of size validation while unpacking frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.5	More Details
CVE-2022-22065	Out of bound read in WLAN HOST due to improper length check can lead to DOS in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.5	More Details
CVE-2022-22083	Denial of service due to memory corruption while extracting ape header from clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.5	More Details
CVE-2022-30937	A vulnerability has been identified in EN100 Ethernet module DNP3 IP variant (All versions), EN100 Ethernet module IEC 104 variant (All versions), EN100 Ethernet module IEC 61850 variant (All versions < V4.37), EN100 Ethernet module Modbus TCP variant (All versions), EN100 Ethernet module PROFINET IO variant (All versions). Affected applications contains a memory corruption vulnerability while parsing specially crafted HTTP packets to /txtrace endpoint. This could allow an attacker to crash the affected application leading to a denial of service condition.	7.5	More Details
CVE-2022-32285	A vulnerability has been identified in Mendix SAML Module (Mendix 7 compatible) (All versions < V1.16.6), Mendix SAML Module (Mendix 8 compatible) (All versions < V2.2.2), Mendix SAML Module (Mendix 9 compatible) (All versions < V3.2.3). The affected module is vulnerable to XML External Entity (XXE) attacks due to insufficient input sanitation. This may allow an attacker to disclose confidential data under certain circumstances.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31308	A vulnerability in live_mfg.shtml of WAVLINK AERIAL X 1200M M79X3.V5030.191012 allows attackers to obtain sensitive router information via execution of the exec cmd function.	7.5	More Details
CVE-2022-32558	An issue was discovered in Couchbase Server before 7.0.4. Sample bucket loading may leak internal user passwords during a failure.	7.5	More Details
CVE-2022-31309	A vulnerability in live_check.shtml of WAVLINK AERIAL X 1200M M79X3.V5030.180719 allows attackers to obtain sensitive router information via execution of the exec cmd function.	7.5	More Details
CVE-2022-31845	A vulnerability in live_check.shtml of WAVLINK WN535 G3 M35G3R.V5030.180927 allows attackers to obtain sensitive router information via execution of the exec cmd function.	7.5	More Details
CVE-2022-31846	A vulnerability in live_mfg.shtml of WAVLINK WN535 G3 M35G3R.V5030.180927 allows attackers to obtain sensitive router information via execution of the exec cmd function.	7.5	More Details
CVE-2022-31847	A vulnerability in /cgi-bin/ExportAllSettings.sh of WAVLINK WN579 X3 M79X3.V5030.180719 allows attackers to obtain sensitive router information via a crafted POST request.	7.5	More Details
CVE-2022-32557	An issue was discovered in Couchbase Server before 7.0.4. The Index Service does not enforce authentication for TCP/TLS servers.	7.5	More Details
CVE-2022-32230	Microsoft Windows SMBv3 suffers from a null pointer dereference in versions of Windows prior to the April, 2022 patch set. By sending a malformed FileNormalizedNameInformation SMBv3 request over a named pipe, an attacker can cause a Blue Screen of Death (BSOD) crash of the Windows kernel. For most systems, this attack requires authentication, except in the special case of Windows Domain Controllers, where unauthenticated users can always open named pipes as long as they can establish an SMB session. Typically, after the BSOD, the victim SMBv3 server will reboot.	7.5	More Details
CVE-2021-35111	Improper validation of tag id while RRC sending tag id to MAC can lead to TOCTOU race condition in Snapdragon Connectivity, Snapdragon Mobile	7.5	More Details
CVE-2021-35100	Possible buffer over read due to improper calculation of string length while parsing Id3 tag in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.5	More Details
CVE-2021-35096	Improper memory allocation during counter check DLM handling can lead to denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2021-35087	Possible null pointer access due to improper validation of system information message to be processed in Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2021-35086	Possible buffer over read due to improper validation of SIB type when processing a NR system Information message in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2021-35078	Possible memory leak due to improper validation of certificate chain length while parsing server certificate chain in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35076	Possible null pointer dereference due to improper validation of RRC connection reconfiguration message in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2021-35073	Possible assertion due to improper validation of rank restriction field in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2021-30344	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.5	More Details
CVE-2021-30340	Reachable assertion due to improper validation of coreset in PDCCH configuration in SA mode in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2021-30327	Buffer overflow in sahara protocol while processing commands leads to overwrite of secure configuration data in Snapdragon Mobile, Snapdragon Compute, Snapdragon Auto, Snapdragon IOT, Snapdragon Connectivity, Snapdragon Voice & Music	7.5	More Details
CVE-2022-29509	Directory traversal vulnerability in T&D Data Server (Japanese Edition) Ver.2.22 and earlier, T&D Data Server (English Edition) Ver.2.30 and earlier, THERMO RECORDER DATA SERVER (Japanese Edition) Ver.2.13 and earlier, and THERMO RECORDER DATA SERVER (English Edition) Ver.2.13 and earlier allows a remote attacker to view an arbitrary file on the server via unspecified vectors.	7.5	More Details
CVE-2022-31447	An XML external entity (XXE) injection vulnerability in Magicpin v3.4 allows attackers to access sensitive database information via a crafted SVG file.	7.5	More Details
CVE-2022-32565	An issue was discovered in Couchbase Server before 7.0.4. The Backup Service log leaks unredacted usernames and document ids.	7.5	More Details
CVE-2022-32192	Couchbase Server 5.x through 7.x before 7.0.4 exposes Sensitive Information to an Unauthorized Actor.	7.5	More Details
CVE-2022-32564	An issue was discovered in Couchbase Server before 7.0.4. In couchbase-cli, server-eshell leaks the Cluster Manager cookie.	7.5	More Details
CVE-2022-32560	An issue was discovered in Couchbase Server before 7.0.4. XDCR lacks role checking when changing internal settings.	7.5	More Details
CVE-2018-17240	There is a memory dump vulnerability on Netwave IP camera devices at //proc/kcore that allows an unauthenticated attacker to exfiltrate sensitive information from the network configuration (e.g., username and password).	7.5	More Details
CVE-2022-29244	npm pack ignores root-level .gitignore and .npmignore file exclusion directives when run in a workspace or with a workspace flag (ie. `--workspaces`, `--workspace=<name>`). Anyone who has run `npm pack` or `npm publish` inside a workspace, as of v7.9.0 and v7.13.0 respectively, may be affected and have published files into the npm registry they did not intend to include. Users should upgrade to the latest, patched version of npm v8.11.0, run: npm i -g npm@latest . Node.js versions v16.15.1, v17.19.1, and v18.3.0 include the patched v8.11.0 version of npm.	7.5	More Details
CVE-2022-29228	Envoy is a cloud-native high-performance proxy. In versions prior to 1.22.1 the OAuth filter would try to invoke the remaining filters in the chain after emitting a local response, which triggers an ASSERT() in newer versions and corrupts memory on earlier versions. continueDecoding() shouldn't ever be called from filters after a local reply has been sent. Users are advised to upgrade. There are no known workarounds for this issue.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26377	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.	7.5	More Details
CVE-2022-29225	Envoy is a cloud-native high-performance proxy. In versions prior to 1.22.1 secompressors accumulate decompressed data into an intermediate buffer before overwriting the body in the decode/encodeBody. This may allow an attacker to zip bomb the decompressor by sending a small highly compressed payload. Maliciously constructed zip files may exhaust system memory and cause a denial of service. Users are advised to upgrade. Users unable to upgrade may consider disabling decompression.	7.5	More Details
CVE-2022-29404	In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.	7.5	More Details
CVE-2022-31042	Guzzle is an open source PHP HTTP client. In affected versions the `Cookie` headers on requests are sensitive information. On making a request using the `https` scheme to a server which responds with a redirect to a URI with the `http` scheme, or on making a request to a server which responds with a redirect to a a URI to a different host, we should not forward the `Cookie` header on. Prior to this fix, only cookies that were managed by our cookie middleware would be safely removed, and any `Cookie` header manually added to the initial request would not be stripped. We now always strip it, and allow the cookie middleware to re-add any cookies that it deems should be there. Affected Guzzle 7 users should upgrade to Guzzle 7.4.4 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.7 or 7.4.4. Users unable to upgrade may consider an alternative approach to use your own redirect middleware, rather than ours. If you do not require or expect redirects to be followed, one should simply disable redirects all together.	7.5	More Details
CVE-2022-30522	If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort.	7.5	More Details
CVE-2017-20022	A vulnerability has been found in Solare Solar-Log 2.8.4-56/3.5.2-85 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to information disclosure. The attack can be initiated remotely. Upgrading to version 3.5.3-86 is able to address this issue. It is recommended to upgrade the affected component.	7.5	More Details
CVE-2022-23138	ZTE's MF297D product has cryptographic issues vulnerability. Due to the use of weak random values, the security of the device is reduced, and it may face the risk of attack.	7.5	More Details
CVE-2022-30556	Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.	7.5	More Details
CVE-2022-29227	Envoy is a cloud-native high-performance edge/middle/service proxy. In versions prior to 1.22.1 if Envoy attempts to send an internal redirect of an HTTP request consisting of more than HTTP headers, there's a lifetime bug which can be triggered. If while replaying the request Envoy sends a local reply when the redirect headers are processed, the downstream state indicates that the downstream stream is not complete. On sending the local reply, Envoy will attempt to reset the upstream stream, but as it is actually complete, and deleted, this result in a use-after-free. Users are advised to upgrade. Users unable to upgrade are advised to disable internal redirects if crashes are observed.	7.5	More Details
CVE-2022-29014	A local file inclusion vulnerability in Razer Sila Gaming Router v2.0.441_api-2.0.418 allows attackers to read arbitrary files.	7.5	More Details
CVE-2022-31019	Vapor is a server-side Swift HTTP web framework. When using automatic content decoding an attacker can craft a request body that can make the server crash with the following request: `curl -d "array[_0][0][array][_0][0][array]$(for f in $(seq 1100); do echo -n '[_0][0][array]'; done)[string][_0]=hello%20world" http://localhost:8080/foo`. The issue is unbounded, attacker controlled stack growth which will at some point lead to a stack overflow and a process crash. This issue has been fixed in version 4.61.1.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25151	Within the Service Desk module of the ITarian platform (SAAS and on-premise), a remote attacker can obtain sensitive information, caused by the failure to set the HTTP Only flag. A remote attacker could exploit this vulnerability to gain access to the management interface by using this vulnerability in combination with a successful Cross-Site Scripting attack on a user.	7.5	More Details
CVE-2022-31043	Guzzle is an open source PHP HTTP client. In affected versions `Authorization` headers on requests are sensitive information. On making a request using the `https` scheme to a server which responds with a redirect to a URI with the `http` scheme, we should not forward the `Authorization` header on. This is much the same as to how we don't forward on the header if the host changes. Prior to this fix, `https` to `http` downgrades did not result in the `Authorization` header being removed, only changes to the host. Affected Guzzle 7 users should upgrade to Guzzle 7.4.4 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.7 or 7.4.4. Users unable to upgrade may consider an alternative approach which would be to use their own redirect middleware. Alternately users may simply disable redirects all together if redirects are not expected or required.	7.5	More Details
CVE-2017-20045	A vulnerability was found in Navetti PricePoint 4.6.0.0. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.7.0.0 is able to address this issue. It is recommended to upgrade the affected component.	7.3	More Details
CVE-2022-22086	Memory corruption in video due to double free while parsing 3gp clip with invalid meta data atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.3	More Details
CVE-2016-15002	A vulnerability, which was classified as critical, was found in MONyog Ultimate 6.63. This affects an unknown part of the component Cookie Handler. The manipulation of the argument HasServerEdit/IsAdmin leads to privilege escalation. It is possible to initiate the attack remotely.	7.3	More Details
CVE-2017-20025	A vulnerability was found in Solare Solar-Log 2.8.4-56/3.5.2-85. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Flash Memory. The manipulation leads to privilege escalation. The attack can be launched remotely. Upgrading to version 3.5.3-86 is able to address this issue. It is recommended to upgrade the affected component.	7.3	More Details
CVE-2022-2019	A vulnerability classified as critical was found in SourceCodester Prison Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /classes/Users.php?f=save of the component New User Creation. The manipulation leads to improper authorization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2017-20029	A vulnerability was found in PHPList 3.2.6 and classified as critical. This issue affects some unknown processing of the file /lists/index.php of the component Edit Subscription. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.3.1 is able to address this issue. It is recommended to upgrade the affected component.	7.3	More Details
CVE-2022-22087	memory corruption in video due to buffer overflow while parsing mkv clip with no codechecker in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.3	More Details
CVE-2022-32350	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/classes/Master.php?f=delete_room_type.	7.2	More Details
CVE-2022-32365	Product Show Room Site v1.0 is vulnerable to SQL Injection via /psrs/admin/fields/manage_field.php?id=.	7.2	More Details
CVE-2022-32364	Product Show Room Site v1.0 is vulnerable to SQL Injection via /psrs/admin/?page=products/manage_product&id=.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32348	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/classes/Master.php?f=delete_doctor.	7.2	More Details
CVE-2022-32349	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/classes/Master.php?f=delete_patient_history.	7.2	More Details
CVE-2022-32351	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/classes/Master.php?f=delete_message.	7.2	More Details
CVE-2022-32366	Product Show Room Site v1.0 is vulnerable to SQL Injection via /psrs/admin/fields/view_field.php?id=.	7.2	More Details
CVE-2022-32367	Product Show Room Site v1.0 is vulnerable to SQL Injection via /psrs/admin/?page=inquiries/view_inquiry&id=.	7.2	More Details
CVE-2022-32347	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/classes/Master.php?f=delete_room.	7.2	More Details
CVE-2022-32346	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/admin/rooms/view_room.php?id=.	7.2	More Details
CVE-2022-32334	Fast Food Ordering System v1.0 is vulnerable to SQL Injection via /ffos/admin/categories/manage_category.php?id=.	7.2	More Details
CVE-2022-32335	Fast Food Ordering System v1.0 is vulnerable to SQL Injection via /ffos/admin/menus/manage_menu.php?id=.	7.2	More Details
CVE-2022-32331	Fast Food Ordering System v1.0 is vulnerable to SQL Injection via /ffos/admin/categories/view_category.php?id=.	7.2	More Details
CVE-2022-32338	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/admin/doctors/manage_doctor.php?id=.	7.2	More Details
CVE-2022-32330	Fast Food Ordering System v1.0 is vulnerable to SQL Injection via /ffos/classes/Master.php?f=delete_menu.	7.2	More Details
CVE-2022-32339	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/admin/doctors/view_doctor.php?id=.	7.2	More Details
CVE-2022-32340	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/admin/?page=patients/view_patient&id=.	7.2	More Details
CVE-2022-1800	The Export any WordPress data to XML/CSV WordPress plugin before 1.3.5 does not sanitize the cpt POST parameter when exporting post data before using it in a database query, leading to an SQL injection vulnerability.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32341	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/admin/?page=user/manage_user&id=.	7.2	More Details
CVE-2022-32342	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/admin/room_types/view_room_type.php?id=.	7.2	More Details
CVE-2022-32343	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via hprms/admin/room_types/manage_room_type.php?id=.	7.2	More Details
CVE-2022-32344	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/classes/Master.php?f=delete_patient.	7.2	More Details
CVE-2022-32345	Hospital's Patient Records Management System v1.0 is vulnerable to SQL Injection via /hprms/admin/rooms/manage_room.php?id=.	7.2	More Details
CVE-2022-0863	The WP SVG Icons WordPress plugin through 3.2.3 does not properly validate uploaded custom icon packs, allowing an high privileged user like an admin to upload a zip file containing malicious php code, leading to remote code execution.	7.2	More Details
CVE-2022-28704	Improper access control vulnerability in Rakuten Casa version AP_F_V1_4_1 or AP_F_V2_0_0 allows a remote attacker to log in with the root privilege and perform an arbitrary operation if the product is in its default settings in which is set to accept SSH connections from the WAN side, and is also connected to the Internet with the authentication information unchanged from the default settings.	7.2	More Details
CVE-2022-32332	Fast Food Ordering System v1.0 is vulnerable to SQL Injection via /ffos/classes/Master.php?f=delete_category.	7.2	More Details
CVE-2022-32333	Fast Food Ordering System v1.0 is vulnerable to SQL Injection via /ffos/admin/sales/receipt.php?id=.	7.2	More Details
CVE-2022-32359	Product Show Room Site v1.0 is vulnerable to SQL Injection via /psrs/classes/Master.php?f=delete_category.	7.2	More Details
CVE-2022-32358	Product Show Room Site v1.0 is vulnerable to SQL Injection via /psrs/classes/Master.php?f=delete_inquiry.	7.2	More Details
CVE-2022-32355	Product Show Room Site v1.0 is vulnerable to SQL Injection via /psrs/admin/?page=products/view_product&id=.	7.2	More Details
CVE-2022-24376	All versions of package git-promise are vulnerable to Command Injection due to an inappropriate fix of a prior [vulnerability](https://security.snyk.io/vuln/SNYK-JS-GITPROMISE-567476) in this package. **Note:** Please note that the vulnerability will not be fixed. The README file was updated with a warning regarding this issue.	7.2	More Details
CVE-2022-32354	Product Show Room Site v1.0 is vulnerable to SQL Injection via /psrs/admin/?page=user/manage_user&id=.	7.2	More Details
CVE-2022-32363	Product Show Room Site v1.0 is vulnerable to SQL Injection via /psrs/admin/categories/view_category.php?id=.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31325	There is a SQL Injection vulnerability in ChurchCRM 4.4.5 via the 'PersonID' field in /churchcrm/WhyCameEditor.php.	7.2	More Details
CVE-2022-32362	Product Show Room Site v1.0 is vulnerable to SQL Injection via /psrs/admin/categories/manage_category.php?id=.	7.2	More Details
CVE-2022-32353	Product Show Room Site v1.0 is vulnerable to SQL Injection via /psrs/admin/categories/manage_field_order.php?id=.	7.2	More Details
CVE-2022-31040	Open Forms is an application for creating and publishing smart forms. Prior to versions 1.0.9 and 1.1.1, the cookie consent page in Open Forms contains an open redirect by injecting a `referer` querystring parameter and failing to validate the value. A malicious actor is able to redirect users to a website under their control, opening them up for phishing attacks. The redirect is initiated by the open forms backend which is a legimate page, making it less obvious to end users they are being redirected to a malicious website. Versions 1.0.9 and 1.1.1 contain patches for this issue. There are no known workarounds avaialble.	7.1	More Details
CVE-2021-30338	Improper input validation in TrustZone memory transfer interface can lead to information disclosure in Snapdragon Compute	7.1	More Details
CVE-2022-29093	Dell SupportAssist Client Consumer versions (3.10.4 and versions prior) and Dell SupportAssist Client Commercial versions (3.1.1 and versions prior) contain an arbitrary file deletion vulnerability. Authenticated non-admin user could exploit the issue and delete arbitrary files on the system.	7.1	More Details
CVE-2022-29094	Dell SupportAssist Client Consumer versions (3.10.4 and versions prior) and Dell SupportAssist Client Commercial versions (3.1.1 and versions prior) contain an arbitrary file deletion/overwrite vulnerability. Authenticated non-admin user could exploit the issue and delete or overwrite arbitrary files on the system.	7.1	More Details
CVE-2021-35101	Improper handling of writes to virtual GICR control can lead to assertion failure in the hypervisor in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile	7.1	More Details
CVE-2022-29241	Jupyter Server provides the backend (i.e. the core services, APIs, and REST endpoints) for Jupyter web applications like Jupyter Notebook. Prior to version 1.17.1, if notebook server is started with a value of `root_dir` that contains the starting user's home directory, then the underlying REST API can be used to leak the access token assigned at start time by guessing/brute forcing the PID of the jupyter server. While this requires an authenticated user session, this URL can be used from a cross-site scripting payload or from a hooked or otherwise compromised browser to leak this access token to a malicious third party. This token can be used along with the REST API to interact with Jupyter services/notebooks such as modifying or overwriting critical files, such as .bashrc or .ssh/authorized_keys, allowing a malicious user to read potentially sensitive data and possibly gain control of the impacted system. This issue is patched in version 1.17.1.	7.1	More Details
CVE-2022-31045	Istio is an open platform to connect, manage, and secure microservices. In affected versions ill-formed headers sent to Envoy in certain configurations can lead to unexpected memory access resulting in undefined behavior or crashing. Users are most likely at risk if they have an Istio ingress Gateway exposed to external traffic. This vulnerability has been resolved in versions 1.12.8, 1.13.5, and 1.14.1. Users are advised to upgrade. There are no known workarounds for this issue.	7.0	More Details
CVE-2022-28383	An issue was discovered in certain Verbatim drives through 2022-03-31. Due to insufficient firmware validation, an attacker can store malicious firmware code for the USB-to-SATA bridge controller on the USB drive (e.g., by leveraging physical access during the supply chain). This code is then executed. This affects Keypad Secure USB 3.2 Gen 1 Drive Part Number #49428, Store 'n' Go Secure Portable HDD GD25LK01-3637-C VER4.0, Executive Fingerprint Secure SSD GDMSFE01-INI3637-C VER1.1, and Fingerprint Secure Portable Hard Drive Part Number #53650.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22259	There is an improper authentication vulnerability in FLMG-10 10.0.1.0(H100SP22C00). Successful exploitation of this vulnerability may lead to a control of the victim device.	6.8	More Details
CVE-2021-35120	Improper handling between export and release functions on the same handle from client can lead to use after free in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	6.7	More Details
CVE-2021-35098	Improper validation of session id in PCM routing process can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.7	More Details
CVE-2021-35092	Processing DCB/AVB algorithm with an invalid queue index from IOCTL request could lead to arbitrary address modification in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	6.7	More Details
CVE-2022-31594	A highly privileged user can exploit SUID-root program to escalate his privileges to root on a local Unix system.	6.7	More Details
CVE-2022-26364	x86 pv: Insufficient care with non-coherent mappings T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Xen maintains a type reference count for pages, in addition to a regular reference count. This scheme is used to maintain invariants required for Xen's safety, e.g. PV guests may not have direct writeable access to pagetables; updates need auditing by Xen. Unfortunately, Xen's safety logic doesn't account for CPU-induced cache non-coherency; cases where the CPU can cause the content of the cache to be different to the content in main memory. In such cases, Xen's safety logic can incorrectly conclude that the contents of a page is safe.	6.7	More Details
CVE-2022-21499	KGDB and KDB allow read and write access to kernel memory, and thus should be restricted during lockdown. An attacker with access to a serial port could trigger the debugger so it is important that the debugger respect the lockdown mode when/if it is triggered. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	6.7	More Details
CVE-2022-26363	x86 pv: Insufficient care with non-coherent mappings T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Xen maintains a type reference count for pages, in addition to a regular reference count. This scheme is used to maintain invariants required for Xen's safety, e.g. PV guests may not have direct writeable access to pagetables; updates need auditing by Xen. Unfortunately, Xen's safety logic doesn't account for CPU-induced cache non-coherency; cases where the CPU can cause the content of the cache to be different to the content in main memory. In such cases, Xen's safety logic can incorrectly conclude that the contents of a page is safe.	6.7	More Details
CVE-2021-35121	An array index is improperly used to lock and unlock a mutex which can lead to a Use After Free condition In the Synx driver in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	6.7	More Details
CVE-2021-35118	An out-of-bounds write can occur due to an incorrect input check in the camera driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	6.7	More Details
CVE-2022-29257	Electron is a framework for writing cross-platform desktop applications using JavaScript (JS), HTML, and CSS. A vulnerability in versions prior to 18.0.0-beta.6, 17.2.0, 16.2.6, and 15.5.5 allows attackers who have control over a given apps update server / update storage to serve maliciously crafted update packages that pass the code signing validation check but contain malicious code in some components. This kind of attack would require significant privileges in a potential victim's own auto updating infrastructure and the ease of that attack entirely depends on the potential victim's infrastructure security. Electron versions 18.0.0-beta.6, 17.2.0, 16.2.6, and 15.5.5 contain a fix for this issue. There are no known workarounds.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1788	Due to missing checks the Change Uploaded File Permissions WordPress plugin through 4.0.0 is vulnerable to CSRF attacks. This can be used to change the file and folder permissions of any folder. This could be problematic when specific files like ini files are made readable for everyone due to this.	6.5	More Details
CVE-2022-32260	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application creates temporary user credentials for UMC (User Management Component) users. An attacker could use these temporary credentials for authentication bypass in certain scenarios.	6.5	More Details
CVE-2022-30931	Employee Leaves Management System (ELMS) V 2.1 is vulnerable to Cross Site Request Forgery (CSRF) via /myprofile.php.	6.5	More Details
CVE-2021-30345	RPM secure Stream can access any secure resource due to improper SMMU configuration in Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	6.5	More Details
CVE-2021-30346	RPM secure Stream can access any secure resource due to improper SMMU configuration in Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	6.5	More Details
CVE-2021-35070	RPM secure Stream can access any secure resource due to improper SMMU configuration and can lead to information disclosure in Snapdragon Industrial IOT, Snapdragon Mobile	6.5	More Details
CVE-2022-1790	The New User Email Set Up WordPress plugin through 0.5.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details
CVE-2022-1424	The Ask me WordPress theme before 6.8.2 does not perform CSRF checks for any of its AJAX actions, allowing an attacker to trick logged in users to perform various actions on their behalf on the site.	6.5	More Details
CVE-2022-32259	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.1). The system images for installation or update of the affected application contain unit test scripts with sensitive information. An attacker could gain information about testing architecture and also tamper with test configuration.	6.5	More Details
CVE-2022-32252	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.1). The application does not perform the integrity check of the update packages. Without validation, an admin user might be tricked to install a malicious package, granting root privileges to an attacker.	6.5	More Details
CVE-2022-0779	The User Meta WordPress plugin before 2.4.4 does not validate the filepath parameter of its um_show_uploaded_file AJAX action, which could allow low privileged users such as subscriber to enumerate the local files on the web server via path traversal payloads	6.5	More Details
CVE-2022-28217	Some part of SAP NetWeaver (EP Web Page Composer) does not sufficiently validate an XML document accepted from an untrusted source, which allows an adversary to exploit unprotected XML parking at endpoints, and a possibility to conduct SSRF attacks that could compromise system's Availability by causing system to crash.	6.5	More Details
CVE-2022-30228	A vulnerability has been identified in SICAM GridEdge Essential ARM (All versions < V2.6.6), SICAM GridEdge Essential Intel (All versions < V2.6.6), SICAM GridEdge Essential with GDS ARM (All versions < V2.6.6), SICAM GridEdge Essential with GDS Intel (All versions < V2.6.6). The affected software does not apply cross-origin resource sharing (CORS) restrictions for critical operations. In case an attacker tricks a legitimate user into accessing a special resource a malicious request could be executed.	6.5	More Details
CVE-2022-31415	Online Fire Reporting System v1.0 was discovered to contain a SQL injection vulnerability via the GET parameter in /report/list.php.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1570	The Files Download Delay WordPress plugin before 1.0.7 does not have authorisation and CSRF checks when reseting its settings, which could allow any authenticated users, such as subscriber to perform such action.	6.5	More Details
CVE-2022-32193	Couchbase Server 6.6.x through 7.x before 7.0.4 exposes Sensitive Information to an Unauthorized Actor.	6.5	More Details
CVE-2022-30898	A Cross-site request forgery (CSRF) vulnerability in Cscms music portal system v4.2 allows remote attackers to change the administrator's username and password.	6.5	More Details
CVE-2021-40616	thinkcmf v5.1.7 has an unauthorized vulnerability. The attacker can modify the password of the administrator account with id 1 through the background user management group permissions. The use condition is that the background user management group authority is required.	6.5	More Details
CVE-2021-40649	In Connx Version 6.2.0.1269 (20210623), a cookie can be issued by the application and not have the HttpOnly flag set.	6.5	More Details
CVE-2022-1422	The Discy WordPress theme before 5.2 does not check for CSRF tokens in the AJAX action discy_reset_options, allowing an attacker to trick an admin into resetting the site settings back to defaults.	6.5	More Details
CVE-2021-40650	In Connx Version 6.2.0.1269 (20210623), a cookie can be issued by the application and not have the secure flag set.	6.5	More Details
CVE-2022-25805	An issue was discovered in the IGEL Universal Management Suite (UMS) 6.07.100. The transmission of cleartext LDAP bind credentials by the cmd_mgt_load_mgt_tree command allows an attacker (who can intercept or inspect traffic between an authenticated UMS client and server) to compromise those LDAP bind credentials.	6.5	More Details
CVE-2021-35080	Disabled SMMU from secure side while RPM is assigned a secure stream can lead to information disclosure in Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	6.5	More Details
CVE-2022-1761	The Peter’s Collaboration E-mails WordPress plugin through 2.2.0 is vulnerable to CSRF due to missing nonce checks. This allows the change of its settings, which can be used to lower the required user level, change texts, the used email address and more.	6.5	More Details
CVE-2022-1694	The Useful Banner Manager WordPress plugin through 1.6.1 does not perform CSRF checks on POST requests to its admin page, allowing an attacker to trick a logged in admin to add, modify or delete banners from the plugin by submitting a form.	6.5	More Details
CVE-2022-1612	The Webriti SMTP Mail WordPress plugin through 1.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details
CVE-2022-0745	The Like Button Rating WordPress plugin before 2.6.45 allows any logged-in user, such as subscriber, to send arbitrary e-mails to any recipient, with any subject and body	6.5	More Details
CVE-2021-25116	The Enqueue Anything WordPress plugin through 1.0.1 does not have authorisation and CSRF checks in the remove_asset AJAX action, and does not ensure that the item to be deleted is actually an asset. As a result, low privilege users such as subscriber could delete arbitrary assets, as well as put arbitrary posts in the trash.	6.5	More Details
CVE-2022-1605	The Email Users WordPress plugin through 4.8.8 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and change the notification settings of arbitrary users	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26041	Directory traversal vulnerability in RCCMD 4.26 and earlier allows a remote authenticated attacker with an administrative privilege to read or alter an arbitrary file on the server via unspecified vectors.	6.5	More Details
CVE-2022-32978	There is an assertion failure in SingleComponentLSScan::ParseMCU in singlecomponentlsscan.cpp in libjpeg before 1.64 via an empty JPEG-LS scan.	6.5	More Details
CVE-2022-1624	The Latest Tweets Widget WordPress plugin through 1.1.4 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details
CVE-2022-31589	Due to improper authorization check, business users who are using Israeli File from SHAAM program (/ATL/VQ23 transaction), are granted more than needed authorization to perform certain transaction, which may lead to users getting access to data that would otherwise be restricted.	6.5	More Details
CVE-2022-31059	Discourse Calendar is a calendar plugin for Discourse, an open-source messaging app. Prior to version 1.0.1, parsing and rendering of Event names can be susceptible to cross-site scripting (XSS) attacks. This vulnerability only affects sites which have modified or disabled Discourse's default Content Security Policy. This issue is patched in version 1.0.1 of the Discourse Calendar plugin. As a workaround, ensure that the Content Security Policy is enabled, and has not been modified in a way which would make it more vulnerable to XSS attacks.	6.5	More Details
CVE-2017-20021	A vulnerability, which was classified as critical, was found in Solare Solar-Log 2.8.4-56/3.5.2-85. This affects an unknown part of the component File Upload. The manipulation leads to privilege escalation. It is possible to initiate the attack remotely. Upgrading to version 3.5.3-86 is able to address this issue. It is recommended to upgrade the affected component.	6.5	More Details
CVE-2022-1608	The OnePress Social Locker WordPress plugin through 5.6.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details
CVE-2022-26362	x86 pv: Race condition in typeref acquisition Xen maintains a type reference count for pages, in addition to a regular reference count. This scheme is used to maintain invariants required for Xen's safety, e.g. PV guests may not have direct writeable access to pagetables; updates need auditing by Xen. Unfortunately, the logic for acquiring a type reference has a race condition, whereby a safely TLB flush is issued too early and creates a window where the guest can re-establish the read/write mapping before writeability is prohibited.	6.4	More Details
CVE-2022-1208	The Ultimate Member plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Biography field featured on individual user profile pages due to insufficient input sanitization and output escaping that allows users to encode malicious web scripts with HTML encoding that is reflected back on the page. This affects versions up to, and including, 2.3.2. Please note this issue was only partially fixed in version 2.3.2.	6.4	More Details
CVE-2017-20032	A vulnerability was found in PHPList 3.2.6. It has been rated as critical. Affected by this issue is some unknown functionality of the component Subscription. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.3.1 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2019-25066	A vulnerability has been found in ajenti 2.1.31 and classified as critical. This vulnerability affects unknown code of the component API. The manipulation leads to privilege escalation. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2.1.32 is able to address this issue. The name of the patch is 7aa146b724e0e20cfee2c71ca78fafbf53a8767c. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2017-20042	A vulnerability has been found in Navetti PricePoint 4.6.0.0 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection (Blind). The attack can be launched remotely. Upgrading to version 4.7.0.0 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-25067	A vulnerability, which was classified as critical, was found in Podman and Varlink 1.5.1. This affects an unknown part of the component API. The manipulation leads to Remote Privilege Escalation. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-143949 was assigned to this vulnerability.	6.3	More Details
CVE-2019-25065	A vulnerability was found in OpenNetAdmin 18.1.1. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to privilege escalation. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2019-25068	A vulnerability classified as critical was found in Axios Italia Axios RE 1.7.0/7.0.0. This vulnerability affects unknown code of the file REDefault.aspx of the component Connection Handler. The manipulation of the argument DBIDX leads to privilege escalation. The attack can be initiated remotely.	6.3	More Details
CVE-2017-20037	A vulnerability has been found in SICUNET Access Controller 0.32-05z and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument c leads to privilege escalation. The attack can be launched remotely.	6.3	More Details
CVE-2017-20023	A vulnerability was found in Solare Solar-Log 2.8.4-56/3.5.2-85 and classified as critical. This issue affects some unknown processing of the component Network Config. The manipulation leads to privilege escalation. The attack may be initiated remotely. Upgrading to version 3.5.3-86 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2017-20017	A vulnerability, which was classified as critical, has been found in The Next Generation of Genealogy Sitebuilding up to 11.1.0. This issue affects some unknown processing of the file /timeline2.php. The manipulation of the argument primaryID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 11.1.1 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2017-20038	A vulnerability was found in SICUNET Access Controller 0.32-05z and classified as critical. Affected by this issue is some unknown functionality of the file card_scan_decoder.php. The manipulation of the argument No/door leads to privilege escalation. The attack may be launched remotely.	6.3	More Details
CVE-2020-36543	A vulnerability, which was classified as critical, was found in SialWeb CMS. This affects an unknown part of the file /about.php. The manipulation of the argument Id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2017-20018	A vulnerability was found in XAMPP 7.1.1-0-VC14. It has been classified as problematic. Affected is an unknown function of the component Installer. The manipulation leads to privilege escalation. It is possible to launch the attack remotely.	6.3	More Details
CVE-2022-0823	An improper control of interaction frequency vulnerability in Zyxel GS1200 series switches could allow a local attacker to guess the password by using a timing side-channel attack.	6.2	More Details
CVE-2021-35079	Improper validation of permissions for third party application accessing Telephony service API can lead to information disclosure in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	6.2	More Details
CVE-2022-1773	The WP Athletics WordPress plugin through 1.1.7 does not sanitise and escape a parameter before outputting back in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-1724	The Simple Membership WordPress plugin before 4.1.1 does not properly sanitise and escape parameters before outputting them back in AJAX actions, leading to Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-0626	The Advanced Admin Search WordPress plugin before 1.1.6 does not sanitize and escape some parameters before outputting them back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31497	LibreHealth EHR Base 2.0.0 allows interface/main/finder/finder_navigation.php patient XSS.	6.1	More Details
CVE-2022-31403	ITOP v3.0.1 was discovered to contain a cross-site scripting (XSS) vulnerability via /itop/pages/ajax.render.php.	6.1	More Details
CVE-2022-32145	A vulnerability has been identified in Teamcenter Active Workspace V5.2 (All versions < V5.2.9), Teamcenter Active Workspace V6.0 (All versions < V6.0.3). A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected application that could allow an attacker to execute malicious code by tricking users into accessing a malicious link.	6.1	More Details
CVE-2022-1241	The Ask me WordPress theme before 6.8.2 does not properly sanitise and escape several of the fields in the Edit Profile page, leading to Reflected Cross-Site Scripting issues	6.1	More Details
CVE-2022-1822	The Zephyr Project Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘project’ parameter in versions up to, and including, 3.2.40 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2022-1005	The WP Statistics WordPress plugin before 13.2.2 does not sanitise the REQUEST_URI parameter before outputting it back in the rendered page, leading to Cross-Site Scripting (XSS) in web browsers which do not encode characters	6.1	More Details
CVE-2022-24969	bypass CVE-2021-25640 > In Apache Dubbo prior to 2.6.12 and 2.7.15, the usage of parseURL method will lead to the bypass of the white host check which can cause open redirect or SSRF vulnerability.	6.1	More Details
CVE-2022-1673	The WooCommerce Green Wallet Gateway WordPress plugin before 1.0.2 does not escape the error_envision query parameter before outputting it to the page, leading to a Reflected Cross-Site Scripting vulnerability.	6.1	More Details
CVE-2022-27231	Cross-site scripting vulnerability exists in WP Statistics versions prior to 13.2.0 because it improperly processes a platform parameter. By exploiting this vulnerability, an arbitrary script may be executed on the web browser of the user who is logging in to the website using the product.	6.1	More Details
CVE-2022-29618	Due to insufficient input validation, SAP NetWeaver Development Infrastructure (Design Time Repository) - versions 7.30, 7.31, 7.40, 7.50, allows an unauthenticated attacker to inject script into the URL and execute code in the user’s browser. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	6.1	More Details
CVE-2021-41663	A cross-site scripting (XSS) vulnerability exists in Mini CMS V1.11. The vulnerability exists in the article upload: post-edit.php page.	6.1	More Details
CVE-2021-41750	A cross-site scripting (XSS) vulnerability in the SEOmatic plugin 3.4.10 for Craft CMS 3 allows remote attackers to inject arbitrary web script via a GET to /index.php?action=seomatic/file/seo-file-link with url parameter containing the base64 encoded URL of a malicious web page / file and fileName parameter containing an arbitrary filename with the intended content-type to be rendered in the user's browser as the extension.	6.1	More Details
CVE-2022-1597	The WPQA Builder WordPress plugin before 5.4, used as a companion for the Discy and Himer , does not sanitise and escape a parameter on its reset password form which makes it possible to perform Reflected Cross-Site Scripting attacks	6.1	More Details
CVE-2022-29485	Cross-site scripting vulnerability in SHIRASAGI v1.0.0 to v1.14.2, and v1.15.0 allows a remote attacker to inject an arbitrary script via unspecified vectors.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2035	A reflected cross-site scripting (XSS) vulnerability exists in the playerConfUrl parameter in the /defaultui/player/modern.html file for SCORM Engine versions < 20.1.45.914, 21.1.x < 21.1.7.219. The issue exists because there are no limitations on the domain or format of the url supplied by the user, allowing an attacker to craft malicious urls which can trigger a reflected XSS payload in the context of a victim's browser.	6.1	More Details
CVE-2022-2066	Cross-site Scripting (XSS) - Reflected in GitHub repository neorazorx/facturascripts prior to 2022.06.	6.1	More Details
CVE-2022-1604	The MailerLite WordPress plugin before 1.5.4 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-1532	Themify WordPress plugin before 1.3.8 does not sanitise and escape the page parameter before outputting it back in an attribute in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-30875	Dolibarr 12.0.5 is vulnerable to Cross Site Scripting (XSS) via Sql Error Page.	6.1	More Details
CVE-2022-1820	The Keep Backup Daily plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘t’ parameter in versions up to, and including, 2.0.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2022-32195	Open edX platform before 2022-06-06 allows XSS via the "next" parameter in the logout URL.	6.1	More Details
CVE-2022-1756	The Newsletter WordPress plugin before 7.4.5 does not sanitize and escape the $_SERVER['REQUEST_URI'] before echoing it back in admin pages. Although this uses addslashes, and most modern browsers automatically URLEncode requests, this is still vulnerable to Reflected XSS in older browsers such as Internet Explorer 9 or below.	6.1	More Details
CVE-2022-1707	The Google Tag Manager for WordPress plugin for WordPress is vulnerable to reflected Cross-Site Scripting via the s parameter due to the site search populating into the data layer of sites with insufficient sanitization in versions up to an including 1.15. The affected file is ~/public/frontend.php and this could be exploited by unauthenticated attackers.	6.1	More Details
CVE-2022-31402	ITOP v3.0.1 was discovered to contain a cross-site scripting (XSS) vulnerability via /itop/webservices/export-v2.php.	6.1	More Details
CVE-2022-32286	A vulnerability has been identified in Mendix SAML Module (Mendix 7 compatible) (All versions < V1.16.6), Mendix SAML Module (Mendix 8 compatible) (All versions < V2.2.2), Mendix SAML Module (Mendix 9 compatible) (All versions < V3.2.3). In certain configurations SAML module is vulnerable to Cross Site Scripting (XSS) attacks due to insufficient error message sanitation. This could allow an attacker to execute malicious code by tricking users into accessing a malicious link.	6.1	More Details
CVE-2021-44266	GUnet Open eClass (aka openeclass) before 3.12.2 allows XSS via the modules/auth/formuser.php auth parameter.	6.1	More Details
CVE-2022-1985	The Download Manager Plugin for WordPress is vulnerable to reflected Cross-Site Scripting in versions up to, and including 3.2.42. This is due to insufficient input sanitization and output escaping on the 'frameid' parameter found in the ~/src/Package/views/shortcode-iframe.php file.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29034	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.1). An error message pop up window in the web interface of the affected application does not prevent injection of JavaScript code. This could allow attackers to perform reflected cross-site scripting (XSS) attacks.	6.1	More Details
CVE-2022-31050	TYPO3 is an open source web content management system. Prior to versions 9.5.34 ELTS, 10.4.29, and 11.5.11, Admin Tool sessions initiated via the TYPO3 backend user interface had not been revoked even if the corresponding user account was degraded to lower permissions or disabled completely. This way, sessions in the admin tool theoretically could have been prolonged without any limit. TYPO3 versions 9.5.34 ELTS, 10.4.29, and 11.5.11 contain a fix for the problem.	6.0	More Details
CVE-2022-31066	EdgeX Foundry is an open source project for building a common open framework for Internet of Things edge computing. Prior to version 2.1.1, the /api/v2/config endpoint exposes message bus credentials to local unauthenticated users. In security-enabled mode, message bus credentials are supposed to be kept in the EdgeX secret store and require authentication to access. This vulnerability bypasses the access controls on message bus credentials when running in security-enabled mode. (No credentials are required when running in security-disabled mode.) As a result, attackers could intercept data or inject fake data into the EdgeX message bus. Users should upgrade to EdgeXFoundry Kamakura release (2.2.0) or to the June 2022 EdgeXFoundry LTS Jakarta release (2.1.1) to receive a patch. More information about which go modules, docker containers, and snaps contain patches is available in the GitHub Security Advisory. There are currently no known workarounds for this issue.	5.9	More Details
CVE-2022-27221	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.1). An attacker in machine-in-the-middle could obtain plaintext secret values by observing length differences during a series of guesses in which a string in an HTTP request URL potentially matches an unknown string in an HTTP response body, aka a "BREACH" attack.	5.9	More Details
CVE-2022-21211	This affects all versions of package posix. When invoking the toString method, it will fallback to 0x0 value, as the value of toString is not invokable (not a function), and then it will crash with type-check.	5.9	More Details
CVE-2017-20040	A vulnerability was found in SICUNET Access Controller 0.32-05z. It has been declared as problematic. This vulnerability affects unknown code of the component Password Storage. The manipulation leads to weak encryption. Attacking locally is a requirement.	5.9	More Details
CVE-2022-23168	The attacker could get access to the database. The SQL injection is in the username parameter at the login panel: username: admin'--	5.9	More Details
CVE-2022-23169	attacker needs to craft a SQL payload. the vulnerable parameter is "agentid" must be authenticated to the admin panel.	5.9	More Details
CVE-2022-31026	Trilogy is a client library for MySQL. When authenticating, a malicious server could return a specially crafted authentication packet, causing the client to read and return up to 12 bytes of data from an uninitialized variable in stack memory. Users of the trilogy gem should upgrade to version 2.1.1 This issue can be avoided by only connecting to trusted servers.	5.9	More Details
CVE-2022-29224	Envoy is a cloud-native high-performance proxy. Versions of envoy prior to 1.22.1 are subject to a segmentation fault in the GrpcHealthCheckerImpl. Envoy can perform various types of upstream health checking. One of them uses gRPC. Envoy also has a feature which can “hold” (prevent removal) upstream hosts obtained via service discovery until configured active health checking fails. If an attacker controls an upstream host and also controls service discovery of that host (via DNS, the EDS API, etc.), an attacker can crash Envoy by forcing removal of the host from service discovery, and then failing the gRPC health check request. This will crash Envoy via a null pointer dereference. Users are advised to upgrade to resolve this vulnerability. Users unable to upgrade may disable gRPC health checking and/or replace it with a different health checking type as a mitigation.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31033	The Mechanize library is used for automating interaction with websites. Mechanize automatically stores and sends cookies, follows redirects, and can follow links and submit forms. In versions prior to 2.8.5 the Authorization header is leaked after a redirect to a different port on the same site. Users are advised to upgrade to Mechanize v2.8.5 or later. There are no known workarounds for this issue.	5.9	More Details
CVE-2017-20028	A vulnerability was found in HumHub 0.20.1/1.0.0-beta.3. It has been classified as critical. This affects an unknown part. The manipulation leads to privilege escalation. It is possible to initiate the attack remotely. Upgrading to version 1.0.0 is able to address this issue. It is recommended to upgrade the affected component.	5.6	More Details
CVE-2022-32241	When a user opens manipulated Portable Document Format (.pdf, PDFView.x3d) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	5.5	More Details
CVE-2022-32242	When a user opens manipulated Radiance Picture (.hdr, hdr.x3d) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	5.5	More Details
CVE-2021-35071	Possible buffer over read due to lack of size validation while copying data from DBR buffer to RX buffer and can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	5.5	More Details
CVE-2022-31287	An issue was discovered in Bento4 v1.2. There is an allocation size request error in /Ap4RtpAtom.cpp.	5.5	More Details
CVE-2022-31285	An issue was discovered in Bento4 1.2. The allocator is out of memory in /Source/C++/Core/Ap4Array.h.	5.5	More Details
CVE-2021-35119	Potential out of Bounds read in FIPS event processing due to improper validation of the length from the firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	5.5	More Details
CVE-2022-32240	When a user opens manipulated Jupiter Tesselation (.jt, JTReader.x3d) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	5.5	More Details
CVE-2021-35085	Possible buffer overflow due to lack of buffer length check during management frame Rx handling in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	5.5	More Details
CVE-2021-35084	Possible out of bound read due to lack of length check of data length for a DIAG event in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	5.5	More Details
CVE-2022-31282	Bento4 MP4Dump v1.2 was discovered to contain a segmentation violation via an unknown address at /Source/C++/Core/Ap4DataBuffer.cpp:175.	5.5	More Details
CVE-2022-25807	An issue was discovered in the IGEL Universal Management Suite (UMS) 6.07.100. A hardcoded DES key in the LDAPDesPWEncrypter class allows an attacker, who has discovered encrypted LDAP bind credentials, to decrypt those credentials using a static 8-byte DES key.	5.5	More Details
CVE-2022-32239	When a user opens manipulated JPEG 2000 (.jp2, jp2k.x3d) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40592	GPAC version before commit 71460d72ec07df766dab0a4d52687529f3efcf0a (version v1.0.1 onwards) contains loop with unreachable exit condition ('infinite loop') vulnerability in ISOBMFF reader filter, isoffin_read.c. Function isoffin_process() can result in DoS by infinite loop. To exploit, the victim must open a specially crafted mp4 file.	5.5	More Details
CVE-2022-30552	Das U-Boot 2022.01 has a Buffer Overflow.	5.5	More Details
CVE-2022-31030	containerd is an open source container runtime. A bug was found in the containerd's CRI implementation where programs inside a container can cause the containerd daemon to consume memory without bound during invocation of the `ExecSync` API. This can cause containerd to consume all available memory on the computer, denying service to other legitimate workloads. Kubernetes and crictl can both be configured to use containerd's CRI implementation; `ExecSync` may be used when running probes or when executing processes via an "exec" facility. This bug has been fixed in containerd 1.6.6 and 1.5.13. Users should update to these versions to resolve the issue. Users unable to upgrade should ensure that only trusted images and commands are used.	5.5	More Details
CVE-2022-25804	An issue was discovered in the IGEL Universal Management Suite (UMS) 6.07.100. Insecure permissions for the serverconfig registry key (under JavaSoft\Prefs\de\igel\rm\config in HKEY_LOCAL_MACHINE\SOFTWARE) allow an unprivileged local attacker to read the encrypted dbuser and dbpassword values for the UMS superuser.	5.5	More Details
CVE-2022-1750	The Sticky Popup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘ popup_title' parameter in versions up to, and including, 1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with admin level capabilities and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This issue mostly affects sites where unfiltered_html has been disabled for administrators and on multi-site installations where unfiltered_html is disabled for administrators.	5.5	More Details
CVE-2022-1961	The Google Tag Manager for WordPress (GTM4WP) plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the `gtm4wp-options[scroller-contentid]` parameter found in the `~/public/frontend.php` file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.15.1. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	5.5	More Details
CVE-2022-30702	Trend Micro Security 2022 and 2021 (Consumer) is vulnerable to an Out-Of-Bounds Read Information Disclosure vulnerability that could allow an attacker to disclose sensitive information on an affected machine.	5.5	More Details
CVE-2022-31751	The kernel emcom module has multi-thread contention. Successful exploitation of this vulnerability may affect system availability.	5.5	More Details
CVE-2022-31755	The communication module has a vulnerability of improper permission preservation. Successful exploitation of this vulnerability may affect system availability.	5.5	More Details
CVE-2022-31756	The fingerprint sensor module has design defects. Successful exploitation of this vulnerability may affect data confidentiality.	5.5	More Details
CVE-2022-31759	AppLink has a vulnerability of accessing uninitialized pointers. Successful exploitation of this vulnerability may affect system availability.	5.5	More Details
CVE-2022-31763	The kernel module has the null pointer and out-of-bounds array vulnerabilities. Successful exploitation of this vulnerability may affect system availability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31752	Missing authorization vulnerability in the system components. Successful exploitation of this vulnerability will affect confidentiality.	5.5	More Details
CVE-2022-21504	The code in UEK6 U3 was missing an appropiate file descriptor count to be missing. This resulted in a use count error that allowed a file descriptor to a socket to be closed and freed while it was still in use by another portion of the kernel. An attack with local access can operate on the socket, and cause a denial of service. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.5	More Details
CVE-2022-28384	An issue was discovered in certain Verbatim drives through 2022-03-31. Due to an insecure design, they allow an offline brute-force attack for determining the correct passcode, and thus gaining unauthorized access to the stored encrypted data. This affects Keypad Secure USB 3.2 Gen 1 Drive Part Number #49428 and Store 'n' Go Secure Portable HDD GD25LK01-3637-C VER4.0.	5.5	More Details
CVE-2022-32235	When a user opens manipulated AutoCAD (.dwg, TeighaTranslator.exe) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	5.5	More Details
CVE-2022-32236	When a user opens manipulated Windows Bitmap (.bmp, 2d.x3d) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	5.5	More Details
CVE-2022-32237	When a user opens manipulated Computer Graphics Metafile (.cgm, CgmCore.dll) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	5.5	More Details
CVE-2022-32238	When a user opens manipulated Encapsulated Post Script (.eps, ai.x3d) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	5.5	More Details
CVE-2022-32243	When a user opens manipulated Scalable Vector Graphics (.svg, svg.x3d) files received from untrusted sources in SAP 3D Visual Enterprise Viewer, the application crashes and becomes temporarily unavailable to the user until restart of the application.	5.5	More Details
CVE-2022-1577	The Database Backup for WordPress plugin before 2.5.2 does not have CSRF check in place when updating the schedule backup settings, which could allow an attacker to make a logged in admin change them via a CSRF attack. This could lead to cases where attackers can send backup notification emails to themselves, which contain more details. Or disable the automatic backup schedule	5.4	More Details
CVE-2022-2016	Cross-site Scripting (XSS) - Reflected in GitHub repository neorazorx/facturascripts prior to 2022.1.	5.4	More Details
CVE-2022-1506	The WP Born Babies WordPress plugin through 1.0 does not sanitise and escape some of its fields, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks	5.4	More Details
CVE-2022-31049	TYPO3 is an open source web content management system. Prior to versions 9.5.34 ELTS, 10.4.29, and 11.5.11, user submitted content was used without being properly encoded in HTML emails sent to users. The actually affected components were mail clients used to view those messages. TYPO3 versions 9.5.34 ELTS, 10.4.29, and 11.5.11 contain a fix for the problem.	5.4	More Details
CVE-2021-40678	In Piwigo 11.5.0, there exists a persistent cross-site scripting in the single mode function through /admin.php?page=batch_manager&mode=unit.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31048	TYPO3 is an open source web content management system. Prior to versions 8.7.47 ELTS, 9.5.34 ELTS, 10.4.29, and 11.5.11, the Form Designer backend module of the Form Framework is vulnerable to cross-site scripting. A valid backend user account with access to the form module is needed to exploit this vulnerability. TYPO3 versions 8.7.47 ELTS, 9.5.34 ELTS, 10.4.29, and 11.5.11 contain a fix for the problem.	5.4	More Details
CVE-2021-40610	Emlog Pro v 1.0.4 cross-site scripting (XSS) in Emlog Pro background management.	5.4	More Details
CVE-2022-2029	Cross-site Scripting (XSS) - DOM in GitHub repository kromitgmbh/titra prior to 0.77.0.	5.4	More Details
CVE-2022-1780	The LaTeX for WordPress plugin through 3.4.10 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack which could also lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping	5.4	More Details
CVE-2022-1763	Due to missing checks the Static Page eXtended WordPress plugin through 2.1 is vulnerable to CSRF attacks which allows changing the plugin settings, including required user levels for specific features. This could also lead to Stored Cross-Site Scripting due to the lack of escaping in some of the settings	5.4	More Details
CVE-2022-1764	The WP-chgFontSize WordPress plugin through 1.8 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping	5.4	More Details
CVE-2022-2036	Cross-site Scripting (XSS) - Stored in GitHub repository francoisjacquet/rosariosis prior to 9.0.1.	5.4	More Details
CVE-2022-1997	Cross-site Scripting (XSS) - Stored in GitHub repository francoisjacquet/rosariosis prior to 9.0.	5.4	More Details
CVE-2022-1659	Vulnerable versions of the JupiterX Core (<= 2.0.6) plugin register an AJAX action jupiterx_conditional_manager which can be used to call any function in the includes/condition/class-condition-manager.php file by sending the desired function to call in the sub_action parameter. This can be used to view site configuration and logged-in users, modify post conditions, or perform a denial of service attack.	5.4	More Details
CVE-2022-31038	Gogs is an open source self-hosted Git service. In versions of gogs prior to 0.12.9 `DisplayName` does not filter characters input from users, which leads to an XSS vulnerability when directly displayed in the issue list. This issue has been resolved in commit 155cae1d which sanitizes `DisplayName` prior to display to the user. All users of gogs are advised to upgrade. Users unable to upgrade should check their users' display names for malicious characters.	5.4	More Details
CVE-2022-24876	GLPI is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. Kanban is a GLPI view to display Projects, Tickets, Changes or Problems on a task board. In versions prior to 10.0.1 a user can exploit a cross site scripting vulnerability in Kanban by injecting HTML code in its user name. Users are advised to upgrade. There are no known workarounds for this issue.	5.4	More Details
CVE-2022-2060	Cross-site Scripting (XSS) - Stored in GitHub repository dolibarr/dolibarr prior to 16.0.	5.4	More Details
CVE-2022-1781	The postTabs WordPress plugin through 2.10.6 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack, which also lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1787	The Sideblog WordPress plugin through 6.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping	5.4	More Details
CVE-2022-1792	The Quick Subscribe WordPress plugin through 1.7.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and leading to Stored XSS due to the lack of sanitisation and escaping in some of them	5.4	More Details
CVE-2021-41502	An issue was discovered in Subrion CMS v4.2.1 There is a stored cross-site scripting (XSS) vulnerability that can execute malicious JavaScript code by modifying the name of the uploaded image, closing the html tag, or adding the onerror attribute.	5.4	More Details
CVE-2022-2065	Cross-site Scripting (XSS) - Stored in GitHub repository neorazorx/facturascripts prior to 2022.06.	5.4	More Details
CVE-2017-20041	A vulnerability was found in Ucweb UC Browser 11.2.5.932. It has been classified as critical. Affected is an unknown function of the component HTML Handler. The manipulation of the argument title leads to improper restriction of rendered ui layers (URL). It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	5.4	More Details
CVE-2021-40902	flatCore-CMS version 2.0.8 is affected by Cross Site Scripting (XSS) in the "Create New Page" option through the index page.	5.4	More Details
CVE-2022-1549	The WP Athletics WordPress plugin through 1.1.7 does not sanitize parameters before storing them in the database, nor does it escape the values when outputting them back in the admin dashboard, leading to a Stored Cross-Site Scripting vulnerability.	5.4	More Details
CVE-2022-2028	Cross-site Scripting (XSS) - Generic in GitHub repository kromitgmbh/titra prior to 0.77.0.	5.4	More Details
CVE-2022-1658	Vulnerable versions of the Jupiter Theme (<= 6.10.1) allow arbitrary plugin deletion by any authenticated user, including users with the subscriber role, via the abb_remove_plugin AJAX action registered in the framework/admin/control-panel/logic/plugin-management.php file. Using this functionality, any logged-in user can delete any installed plugin on the site.	5.4	More Details
CVE-2022-1759	The RB Internal Links WordPress plugin through 2.0.16 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack, as well as perform Stored Cross-Site Scripting attacks due to the lack of sanitisation and escaping	5.4	More Details
CVE-2022-2026	Cross-site Scripting (XSS) - Stored in GitHub repository kromitgmbh/titra prior to 0.77.0.	5.4	More Details
CVE-2022-2015	Cross-site Scripting (XSS) - Stored in GitHub repository jgraph/drawio prior to 19.0.2.	5.4	More Details
CVE-2022-30611	IBM Spectrum Copy Data Management 2.2.0.0 through 2.2.15.0 is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using some fields of the form in the portal UI to inject malicious script into a Web page which would be executed in a victim's Web browser within the security context of the hosting Web site, once the page is viewed. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials. IBM X-Force ID: 227364.	5.4	More Details
CVE-2022-2014	Code Injection in GitHub repository jgraph/drawio prior to 19.0.2.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1656	Vulnerable versions of the JupiterX Theme (<=2.0.6) allow any logged-in user, including subscriber-level users, to access any of the functions registered in lib/api/api/ajax.php, which also grant access to the jupiterx_api_ajax_ actions registered by the JupiterX Core Plugin (<=2.0.6). This includes the ability to deactivate arbitrary plugins as well as update the theme's API key.	5.4	More Details
CVE-2022-2079	Cross-site Scripting (XSS) - Stored in GitHub repository nocodb/nocodb prior to 0.91.7+.	5.4	More Details
CVE-2022-32258	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.1). The affected application contains an older feature that allows to import device configurations via a specific endpoint. An attacker could use this vulnerability for information disclosure.	5.3	More Details
CVE-2022-32261	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.1). The affected application contains a misconfiguration in the APT update. This could allow an attacker to add insecure packages to the application.	5.3	More Details
CVE-2022-1595	The HC Custom WP-Admin URL WordPress plugin through 1.4 leaks the secret login URL when sending a specific crafted request	5.3	More Details
CVE-2022-32255	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.1). The affected application consists of a web service that lacks proper access control for some of the endpoints. This could lead to unauthorized access to limited information.	5.3	More Details
CVE-2019-25069	A vulnerability, which was classified as problematic, has been found in Axios Italia Axios RE 1.7.0/7.0.0. This issue affects some unknown processing of the component Error Message Handler. The manipulation leads to information disclosure (ASP.NET). The attack may be initiated remotely.	5.3	More Details
CVE-2022-32741	Attacker is able to determine if the provided username exists (and it's valid) using Request New Password feature, based on the response time.	5.3	More Details
CVE-2019-25063	A vulnerability was found in Sricam IP CCTV Camera. It has been classified as critical. Affected is an unknown function of the component Device Viewer. The manipulation leads to memory corruption. Local access is required to approach this attack.	5.3	More Details
CVE-2022-27889	The Multipass service was found to have code paths that could be abused to cause a denial of service for authentication or authorization operations. A malicious attacker could perform an application-level denial of service attack, potentially causing authentication and/or authorization operations to fail for the duration of the attack. This could lead to performance degradation or login failures for customer Palantir Foundry environments. This vulnerability is resolved in Multipass 3.647.0. This issue affects: Palantir Foundry Multipass versions prior to 3.647.0.	5.3	More Details
CVE-2017-20024	A vulnerability was found in Solare Solar-Log 2.8.4-56/3.5.2-85. It has been classified as problematic. Affected is an unknown function. The manipulation leads to denial of service. It is possible to launch the attack remotely. Upgrading to version 3.5.3-86 is able to address this issue. It is recommended to upgrade the affected component.	5.3	More Details
CVE-2022-31060	Discourse is an open-source discussion platform. Prior to version 2.8.4 in the `stable` branch and version `2.9.0.beta5` in the `beta` and `tests-passed` branches, banner topic data is exposed on login-required sites. This issue is patched in version 2.8.4 in the `stable` branch and version `2.9.0.beta5` in the `beta` and `tests-passed` branches of Discourse. As a workaround, one may disable banners.	5.3	More Details
CVE-2017-20020	A vulnerability, which was classified as problematic, has been found in Solare Solar-Log 2.8.4-56/3.5.2-85. Affected by this issue is some unknown functionality. The manipulation leads to cross site request forgery. The attack may be launched remotely. Upgrading to version 3.5.3-86 is able to address this issue. It is recommended to upgrade the affected component.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1598	The WPQA Builder WordPress plugin before 5.5 which is a companion to the Discy and Himer , lacks authentication in a REST API endpoint, allowing unauthenticated users to discover private questions sent between users on the site.	5.3	More Details
CVE-2022-23167	Attacker crafts a GET request to: /mobile/downloadfile.aspx? Filename =../.. /windows/boot.ini the LFI is UNAUTHENTICATED.	5.3	More Details
CVE-2022-28330	Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.	5.3	More Details
CVE-2022-28614	The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.	5.3	More Details
CVE-2019-25062	A vulnerability was found in Sricam IP CCTV Camera and classified as critical. This issue affects some unknown processing of the component Device Viewer. The manipulation leads to memory corruption. An attack has to be approached locally. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2022-31047	TYPO3 is an open source web content management system. Prior to versions 7.6.57 ELTS, 8.7.47 ELTS, 9.5.34 ELTS, 10.4.29, and 11.5.11, system internal credentials or keys (e.g. database credentials) can be logged as plaintext in exception handlers, when logging the complete exception stack trace. TYPO3 versions 7.6.57 ELTS, 8.7.47 ELTS, 9.5.34 ELTS, 10.4.29, 11.5.11 contain a fix for the problem.	5.3	More Details
CVE-2021-46811	HwSEServiceAPP has a vulnerability in permission management. Successful exploitation of this vulnerability may cause disclosure of the Card Production Life Cycle (CPLC) information.	5.3	More Details
CVE-2022-31769	IBM Spectrum Copy Data Management 2.2.0.0 through 2.2.15.0 could allow a remote attacker to view product configuration information stored in PostgreSQL, which could be used in further attacks against the system. IBM X-Force ID: 228219.	5.3	More Details
CVE-2022-30229	A vulnerability has been identified in SICAM GridEdge Essential ARM (All versions < V2.6.6), SICAM GridEdge Essential Intel (All versions < V2.6.6), SICAM GridEdge Essential with GDS ARM (All versions < V2.6.6), SICAM GridEdge Essential with GDS Intel (All versions < V2.6.6). The affected software does not require authenticated access for privileged functions. This could allow an unauthenticated attacker to change data of an user, such as credentials, in case that user's id is known.	5.3	More Details
CVE-2022-29614	SAP startservice - of SAP NetWeaver Application Server ABAP, Application Server Java, ABAP Platform and HANA Database - versions KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, SAPHOSTAGENT 7.22, - on Unix systems, s-bit helper program sapuxuserchk, can be abused physically resulting in a privilege escalation of an attacker leading to low impact on confidentiality and integrity, but a profound impact on availability.	5.0	More Details
CVE-2022-1691	The Realty Workstation WordPress plugin before 1.0.15 does not sanitise and escape the trans_edit parameter before using it in a SQL statement when an agent edit a transaction, leading to an SQL injection	4.9	More Details
CVE-2022-32561	An issue was discovered in Couchbase Server before 6.6.5 and 7.x before 7.0.4. Previous mitigations for CVE-2018-15728 were found to be insufficient when it was discovered that diagnostic endpoints could still be accessed from the network.	4.9	More Details
CVE-2022-32253	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.1). Due to improper input validation, the OpenSSL certificate's password could be printed to a file reachable by an attacker.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1685	The Five Minute Webshop WordPress plugin through 1.3.2 does not properly validate and sanitise the orderby parameter before using it in a SQL statement via the Manage Products admin page, leading to an SQL Injection	4.9	More Details
CVE-2022-0209	The Mitsol Social Post Feed WordPress plugin before 1.11 does not escape some of its settings before outputting them back in attributes, which could allow high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-31400	A cross-site scripting (XSS) vulnerability in /staff/setup/email-addresses of Helpdeskz v2.0.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the email name field.	4.8	More Details
CVE-2022-31398	A cross-site scripting (XSS) vulnerability in /staff/tools/custom-fields of Helpdeskz v2.0.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the email name field.	4.8	More Details
CVE-2021-40658	Textpattern 4.8.7 is affected by a HTML injection vulnerability through “Content>Write>Body”.	4.8	More Details
CVE-2022-1814	The WP Admin Style WordPress plugin through 0.1.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-1335	The Slideshow CK WordPress plugin before 1.4.10 does not sanitize and escape Slide's descriptions, which could allow high-privileged users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed	4.8	More Details
CVE-2022-1772	The Google Places Reviews WordPress plugin before 2.0.0 does not properly escape its Google API key setting, which is reflected on the site's administration panel. A malicious administrator could abuse this bug, in a multisite WordPress configuration, to trick super-administrators into viewing the booby-trapped payload and taking over their account.	4.8	More Details
CVE-2022-1710	The Appointment Hour Booking WordPress plugin before 1.3.56 does not sanitise and escape a settings of its Calendar fields, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.	4.8	More Details
CVE-2022-30903	Nokia "G-2425G-A" Bharti Airtel Routers Hardware version "3FE48299DEAA" Software Version "3FE49362IJHK42" is vulnerable to Cross-Site Scripting (XSS) via the admin->Maintenance>Device Management.	4.8	More Details
CVE-2022-1336	The Carousel CK WordPress plugin through 1.1.0 does not sanitize and escape Slide's descriptions, which could allow high-privileged users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed	4.8	More Details
CVE-2022-1469	The FiboSearch WordPress plugin before 1.17.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-1647	The FormCraft WordPress plugin before 1.2.6 does not sanitise and escape Field Labels, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-30899	A Cross Site Scripting vulnerabilty exists in PartKeepr 1.4.0 via the 'name' field in /api/part_categories.	4.8	More Details
CVE-2022-1569	The Drag & Drop Builder, Human Face Detector, Pre-built Templates, Spam Protection, User Email Notifications & more! WordPress plugin before 1.4.9.4 does not sanitise and escape some of its form fields, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29894	Strapi v3.x.x versions and earlier contain a stored cross-site scripting vulnerability in file upload function. By exploiting this vulnerability, an arbitrary script may be executed on the web browser of the user who is logging in to the product with the administrative privilege.	4.8	More Details
CVE-2022-1541	The Video Slider WordPress plugin before 1.4.8 does not sanitize or escape some of its video settings, which could allow high-privileged users to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2022-1394	The Photo Gallery by 10Web WordPress plugin before 1.6.4 does not properly validate and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed	4.8	More Details
CVE-2022-2017	A vulnerability was found in SourceCodester Prison Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /pms/admin/visits/view_visit.php of the component Visit Handler. The manipulation of the argument id with the input 2%27and%201=2%20union%20select%201,2,3,4,5,6,7,user(),database()--+ leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2022-31758	The kernel module has the race condition vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	4.7	More Details
CVE-2022-29455	DOM-based Reflected Cross-Site Scripting (XSS) vulnerability in Elementor's Elementor Website Builder plugin <= 3.5.5 versions.	4.7	More Details
CVE-2022-2018	A vulnerability classified as critical has been found in SourceCodester Prison Management System 1.0. Affected is an unknown function of the file /admin/?page=inmates/view_inmate of the component Inmate Handler. The manipulation of the argument id with the input 1%27%20and%201=2%20union%20select%201,user(),3,4,5,6,7,8,9,0,database(),2,3,4,5,6,7,8,9,0,1,2,3,4--+ leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2017-20030	A vulnerability was found in PHPList 3.2.6. It has been classified as critical. Affected is an unknown function of the file /lists/admin/ of the component Sending Campain. The manipulation leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.3.1 is able to address this issue. It is recommended to upgrade the affected component.	4.7	More Details
CVE-2022-29948	Due to an insecure design, the Lepin EP-KP001 flash drive through KP001_V19 is vulnerable to an authentication bypass attack that enables an attacker to gain access to the stored encrypted data. Normally, the encrypted disk partition with this data is unlocked by entering the correct passcode (6 to 14 digits) via the keypad and pressing the Unlock button. This authentication is performed by an unknown microcontroller. By replacing this microcontroller on a target device with one from an attacker-controlled Lepin EP-KP001 whose passcode is known, it is possible to successfully unlock the target device and read the stored data in cleartext.	4.6	More Details
CVE-2022-28387	An issue was discovered in certain Verbatim drives through 2022-03-31. Due to an insecure design, they can be unlocked by an attacker who can then gain unauthorized access to the stored data. The attacker can simply use an undocumented IOCTL command that retrieves the correct password. This affects Executive Fingerprint Secure SSD GDMSFE01-INI3637-C VER1.1 and Fingerprint Secure Portable Hard Drive Part Number #53650.	4.6	More Details
CVE-2022-28386	An issue was discovered in certain Verbatim drives through 2022-03-31. The security feature for lockout (e.g., requiring a reformat of the drive after 20 failed unlock attempts) does not work as specified. More than 20 attempts may be made. This affects Keypad Secure USB 3.2 Gen 1 Drive Part Number #49428 and Store 'n' Go Secure Portable HDD GD25LK01-3637-C VER4.0.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28385	An issue was discovered in certain Verbatim drives through 2022-03-31. Due to missing integrity checks, an attacker can manipulate the content of the emulated CD-ROM drive (containing the Windows and macOS client software). The content of this emulated CD-ROM drive is stored as an ISO-9660 image in the hidden sectors of the USB drive, that can only be accessed using special IOCTL commands, or when installing the drive in an external disk enclosure. By manipulating this ISO-9660 image or replacing it with another one, an attacker is able to store malicious software on the emulated CD-ROM drive. This software may get executed by an unsuspecting victim when using the device. For example, an attacker with temporary physical access during the supply chain could program a modified ISO-9660 image on a device that always accepts an attacker-controlled password for unlocking the device. If the attacker later on gains access to the used USB drive, he can simply decrypt all contained user data. Storing arbitrary other malicious software is also possible. This affects Executive Fingerprint Secure SSD GDMSFE01-INI3637-C VER1.1 and Fingerprint Secure Portable Hard Drive Part Number #53650.	4.6	More Details
CVE-2021-27786	Cross-origin resource sharing (CORS) enables browsers to perform cross domain requests in a controlled manner. This request has an Origin header that identifies the domain that is making the initial request and defines the protocol between a browser and server to see if the request is allowed. An attacker can take advantage of this and possibly carry out privileged actions and access sensitive information when the Access-Control-Allow-Credentials is enabled.	4.6	More Details
CVE-2022-30610	IBM Spectrum Copy Data Management 2.2.0.0 through 2.2.15.0 is vulnerable to reverse tabnabbing where it could allow a page linked to from within IBM Spectrum Copy Data Management to rewrite it. An administrator could enter a link to a malicious URL that another administrator could then click. Once clicked, that malicious URL could then rewrite the original page with a phishing page. IBM X-Force ID: 227363.	4.5	More Details
CVE-2022-31051	semantic-release is an open source npm package for automated version management and package publishing. In affected versions secrets that would normally be masked by semantic-release can be accidentally disclosed if they contain characters that are excluded from uri encoding by `encodeURI`. Occurrence is further limited to execution contexts where push access to the related repository is not available without modifying the repository url to inject credentials. Users are advised to upgrade. Users unable to upgrade should ensure that secrets that do not contain characters that are excluded from encoding with `encodeURI` when included in a URL are already masked properly.	4.4	More Details
CVE-2017-20027	A vulnerability was found in HumHub up to 1.0.1 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting (DOM). The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.1.1 is able to address this issue. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2022-27174	Cross-site request forgery (CSRF) vulnerability in Easy Blog for EC-CUBE4 Ver.1.0.1 and earlier allows a remote unauthenticated attacker to hijack the authentication of the administrator and delete a blog article or a category via a specially crafted page.	4.3	More Details
CVE-2022-31046	TYPO3 is an open source web content management system. Prior to versions 7.6.57 ELTS, 8.7.47 ELTS, 9.5.34 ELTS, 10.4.29, and 11.5.11, the export functionality fails to limit the result set to allowed columns of a particular database table. This way, authenticated users can export internal details of database tables they already have access to. TYPO3 versions 7.6.57 ELTS, 8.7.47 ELTS, 9.5.34 ELTS, 10.4.29, 11.5.11 fix the problem described above. In order to address this issue, access to mentioned export functionality is completely denied for regular backend users.	4.3	More Details
CVE-2017-20026	A vulnerability has been found in HumHub up to 1.0.1 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting (Reflected). The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.1.1 is able to address this issue. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2017-20043	A vulnerability was found in Navetti PricePoint 4.6.0.0 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to basic cross site scripting (Persistent). The attack may be launched remotely. Upgrading to version 4.7.0.0 is able to address this issue. It is recommended to upgrade the affected component.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20044	A vulnerability was found in Navetti PricePoint 4.6.0.0. It has been classified as problematic. This affects an unknown part. The manipulation leads to basic cross site scripting (Reflected). It is possible to initiate the attack remotely. Upgrading to version 4.7.0.0 is able to address this issue. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2022-29238	Jupyter Notebook is a web-based notebook environment for interactive computing. Prior to version 6.4.12, authenticated requests to the notebook server with `ContentsManager.allow_hidden = False` only prevented listing the contents of hidden directories, not accessing individual hidden files or files in hidden directories (i.e. hidden files were 'hidden' but not 'inaccessible'). This could lead to notebook configurations allowing authenticated access to files that may reasonably be expected to be disallowed. Because fully authenticated requests are required, this is of relatively low impact. But if a server's root directory contains sensitive files whose only protection from the server is being hidden (e.g. `~/.ssh` while serving $HOME), then any authenticated requests could access files if their names are guessable. Such contexts also necessarily have full access to the server and therefore execution permissions, which also generally grants access to all the same files. So this does not generally result in any privilege escalation or increase in information access, only an additional, unintended means by which the files could be accessed. Version 6.4.12 contains a patch for this issue. There are currently no known workarounds.	4.3	More Details
CVE-2017-20033	A vulnerability classified as problematic has been found in PHPList 3.2.6. This affects an unknown part of the file /lists/admin/. The manipulation of the argument page with the input send\\";><script>alert(8) </script> leads to cross site scripting (Reflected). It is possible to initiate the attack remotely. Upgrading to version 3.3.1 is able to address this issue. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2022-24896	Tuleap is a Free & Open Source Suite to manage software developments and collaboration. In versions prior to 13.7.99.239 Tuleap does not properly verify authorizations when displaying the content of tracker report renderer and chart widgets. Malicious users could use this vulnerability to retrieve the name of a tracker they cannot access as well as the name of the fields used in reports.	4.3	More Details
CVE-2022-30930	Tourism Management System Version: V 3.2 is affected by: Cross Site Request Forgery (CSRF).	4.3	More Details
CVE-2022-32273	As a result of an observable discrepancy in returned messages, OPSWAT MetaDefender Core (MDCore) before 5.1.2 could allow an authenticated user to enumerate filenames on the server.	4.3	More Details
CVE-2022-29612	SAP NetWeaver, ABAP Platform and SAP Host Agent - versions KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, 8.04, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, 8.04, SAPHOSTAGENT 7.22, allows an authenticated user to misuse a function of sapcontrol webfunctionality(startservice) in Kernel which enables malicious users to retrieve information. On successful exploitation, an attacker can obtain technical information like system number or physical address, which is otherwise restricted, causing a limited impact on the confidentiality of the application.	4.3	More Details
CVE-2022-1793	The Private Files WordPress plugin through 0.40 is missing CSRF check when disabling the protection, which could allow attackers to make a logged in admin perform such action via a CSRF attack and make the blog public	4.3	More Details
CVE-2022-1594	The HC Custom WP-Admin URL WordPress plugin through 1.4 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack, allowing them to change the login URL	4.3	More Details
CVE-2022-1709	The Throws SPAM Away WordPress plugin before 3.3.1 does not have CSRF checks in place when deleting comments (either all, spam, or pending), allowing attackers to make a logged in admin delete comments via a CSRF attack	4.3	More Details
CVE-2017-20019	A vulnerability classified as problematic was found in Solare Solar-Log 2.8.4-56/3.5.2-85. Affected by this vulnerability is an unknown functionality of the component Config Handler. The manipulation leads to information disclosure. The attack can be launched remotely. Upgrading to version 3.5.3-86 is able to address this issue. It is recommended to upgrade the affected component.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27219	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.0 SP2). Affected application is missing general HTTP security headers in the web server configured on port 443. This could aid attackers by making the servers more prone to clickjacking, channel downgrade attacks and other similar client-based attack vectors.	4.3	More Details
CVE-2022-27220	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.0 SP2). Affected application is missing general HTTP security headers in the web server configured on port 6220. This could aid attackers by making the servers more prone to clickjacking, channel downgrade attacks and other similar client-based attack vectors.	4.3	More Details
CVE-2022-30760	An Insecure Direct Object Reference (IDOR) issue in fn2Web in ihb eG FlexNow before 2.04.09.016 allows remote authenticated attackers to obtain sensitive student information (final grades, study courses, degrees) by changing the student ID parameter in the HTTP POST request to the FrontControllerSS endpoint.	4.3	More Details
CVE-2022-30231	A vulnerability has been identified in SICAM GridEdge Essential ARM (All versions < V2.6.6), SICAM GridEdge Essential Intel (All versions < V2.6.6), SICAM GridEdge Essential with GDS ARM (All versions < V2.6.6), SICAM GridEdge Essential with GDS Intel (All versions < V2.6.6). The affected software discloses password hashes of other users upon request. This could allow an authenticated user to retrieve another users password hash.	4.3	More Details
CVE-2022-1695	The WP Simple Adsense Insertion WordPress plugin before 2.1 does not perform CSRF checks on updates to its admin page, allowing an attacker to trick a logged in user to manipulate ads and inject arbitrary javascript via submitting a form.	4.3	More Details
CVE-2022-1421	The Discy WordPress theme before 5.2 lacks CSRF checks in some AJAX actions, allowing an attacker to make a logged in admin change arbitrary 's settings including payment methods via a CSRF attack	4.3	More Details
CVE-2022-32254	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.1). A customized HTTP POST request could force the application to write the status of a given user to a log file, exposing sensitive user information that could provide valuable guidance to an attacker.	4.3	More Details
CVE-2019-25064	A vulnerability was found in CoreHR Core Portal up to 27.0.7. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross site request forgery. It is possible to launch the attack remotely. Upgrading to version 27.0.8 is able to address this issue. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2022-32256	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.1). The affected application consists of a web service that lacks proper access control for some of the endpoints. This could lead to low privileged users accessing privileged information.	4.3	More Details
CVE-2022-1712	The LiveSync for WordPress plugin through 1.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31027	OAuthenticator is an OAuth token library for the JupyerHub login handler. CILogonOAuthenticator is provided by the OAuthenticator package, and lets users log in to a JupyterHub via CILogon. This is primarily used to restrict a JupyterHub only to users of a given institute. The allowed_idps configuration trait of CILogonOAuthenticator is documented to be a list of domains that indicate the institutions whose users are authorized to access this JupyterHub. This authorization is validated by ensuring that the *email* field provided to us by CILogon has a *domain* that matches one of the domains listed in `allowed_idps`.If `allowed_idps` contains `berkeley.edu`, you might expect only users with valid current credentials provided by University of California, Berkeley to be able to access the JupyterHub. However, CILogonOAuthenticator does *not* verify which provider is used by the user to login, only the email address provided. So a user can login with a GitHub account that has email set to `<something>@berkeley.edu`, and that will be treated exactly the same as someone logging in using the UC Berkeley official Identity Provider. The patch fixing this issue makes a *breaking change* in how `allowed_idps` is interpreted. It's no longer a list of domains, but configuration representing the `EntityID` of the IdPs that are allowed, picked from the [list maintained by CILogon](https://cilogon.org/idplist/). Users are advised to upgrade.	4.2	More Details
CVE-2022-29254	silverstripe-omnipay is a SilverStripe integration with Omnipay PHP payments library. For a subset of Omnipay gateways (those that use intermediary states like `isNotification()` or `isRedirect()`), if the payment identifier or success URL is exposed it is possible for payments to be prematurely marked as completed without payment being taken. This is mitigated by the fact that most payment gateways hide this information from users, however some issuing banks offer flawed 3DSecure implementations that may inadvertently expose this data. The following versions have been patched to fix this issue: `2.5.2`, `3.0.2`, `3.1.4`, and `3.2.1`. There are no known workarounds for this vulnerability.	3.7	More Details
CVE-2022-29482	'Mobaoku-Auction&Flea Market' App for iOS versions prior to 5.5.16 improperly verifies server certificates, which may allow an attacker to eavesdrop on an encrypted communication via a man-in-the-middle attack.	3.7	More Details
CVE-2017-20036	A vulnerability, which was classified as problematic, was found in PHPList 3.2.6. Affected is an unknown function of the file /lists/admin/ of the component Bounce Rule. The manipulation leads to cross site scripting (Persistent). It is possible to launch the attack remotely. Upgrading to version 3.3.1 is able to address this issue. It is recommended to upgrade the affected component.	3.5	More Details
CVE-2017-20035	A vulnerability, which was classified as problematic, has been found in PHPList 3.2.6. This issue affects some unknown processing of the file /lists/admin/ of the component Subscribe. The manipulation leads to cross site scripting (Persistent). The attack may be initiated remotely. Upgrading to version 3.3.1 is able to address this issue. It is recommended to upgrade the affected component.	3.5	More Details
CVE-2018-25034	A vulnerability, which was classified as problematic, has been found in Thomson TCW710 ST5D.10.05. This issue affects some unknown processing of the file /goform/wlanPrimaryNetwork. The manipulation of the argument ServiceSetIdentifier with the input ><script>alert(1)</script> as part of POST Request leads to basic cross site scripting (Persistent). The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-126695.	3.5	More Details
CVE-2018-25035	A vulnerability, which was classified as problematic, was found in Thomson TCW710 ST5D.10.05. Affected is an unknown function of the file /goform/RGFirewallEL. The manipulation of the argument EmailAddress/SmtpServerName with the input ><script>alert(1)</script> as part of POST Request leads to cross site scripting (Persistent). It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2018-25036	A vulnerability has been found in Thomson TCW710 ST5D.10.05 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /goform/RgTime. The manipulation of the argument TimeServer1/TimeServer2/TimeServer3 with the input ><script>alert(1)</script> as part of POST Request leads to cross site scripting (Persistent). The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-25037	A vulnerability was found in Thomson TCW710 ST5D.10.05 and classified as problematic. Affected by this issue is some unknown functionality of the file /goform/RgDdns. The manipulation of the argument DdnsHostName with the input ><script>alert(1)</script> as part of POST Request leads to cross site scripting (Persistent). The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2018-25038	A vulnerability was found in Thomson TCW710 ST5D.10.05. It has been classified as problematic. This affects an unknown part of the file /goform/RgDhcp. The manipulation of the argument PppUserName with the input ><script>alert(1)</script> as part of POST Request leads to cross site scripting (Persistent). It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2017-20034	A vulnerability classified as problematic was found in PHPList 3.2.6. This vulnerability affects unknown code of the file /lists/admin/ of the component List Name. The manipulation leads to cross site scripting (Persistent). The attack can be initiated remotely. Upgrading to version 3.3.1 is able to address this issue. It is recommended to upgrade the affected component.	3.5	More Details
CVE-2019-25070	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in WolfCMS up to 0.8.3.1. It has been rated as problematic. This issue affects some unknown processing of the file /wolfcms/?/admin/user/add of the component User Add. The manipulation of the argument name leads to basic cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-135125 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2018-25039	A vulnerability was found in Thomson TCW710 ST5D.10.05. It has been declared as problematic. This vulnerability affects unknown code of the file /goform/RgUrlBlock.asp. The manipulation of the argument BasicParentalNewKeyword with the input ><script>alert(1)</script> as part of POST Request leads to cross site scripting (Persistent). The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2020-36544	A vulnerability has been found in SialWeb CMS and classified as problematic. This vulnerability affects unknown code of the component Search Handler. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-32740	A reply to a forwarded email article by a 3rd party could unintensionally expose the email content to the ticket customer under certain circumstances.	3.5	More Details
CVE-2022-32739	When Secure::DisableBanner system configuration has been disabled and agent shares his calendar via public URL, received ICS file contains OTRS release number.	3.5	More Details
CVE-2022-29615	SAP NetWeaver Developer Studio (NWDS) - version 7.50, is based on Eclipse, which contains the logging framework log4j in version 1.x. The application's confidentiality and integrity could have a low impact due to the vulnerabilities associated with version 1.x.	3.4	More Details
CVE-2022-22426	IBM Spectrum Copy Data Management Admin 2.2.0.0 through 2.2.15.0 could allow a local attacker to bypass authentication restrictions, caused by the lack of proper session management. An attacker could exploit this vulnerability to bypass authentication and gain unauthorized access to the Spectrum Copy Data Management catalog which contains metadata. IBM X-Force ID: 223718.	3.3	More Details
CVE-2022-2061	Heap-based Buffer Overflow in GitHub repository hpjansson/chafa prior to 1.12.0.	3.3	More Details
CVE-2021-42811	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in SafeNet KeySecure allows an authenticated user to read arbitrary files from the underlying system on which the product is deployed.	3.3	More Details
CVE-2022-1689	The Note Press WordPress plugin through 0.1.10 does not sanitise and escape the Update parameter before using it in a SQL statement when updating a note via the admin dashboard, leading to an SQL injection	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1684	The Cube Slider WordPress plugin through 1.2 does not sanitise and escape the idslider parameter before using it in various SQL queries, leading to SQL Injections exploitable by high privileged users such as admin	2.7	More Details
CVE-2022-1686	The Five Minute Webshop WordPress plugin through 1.3.2 does not sanitise and escape the id parameter before using it in a SQL statement when editing a product via the admin dashboard, leading to an SQL Injection	2.7	More Details
CVE-2022-1687	The Logo Slider WordPress plugin through 1.4.8 does not sanitise and escape the lsp_slider_id parameter before using it in a SQL statement via the Manage Slider Images admin page, leading to an SQL Injection	2.7	More Details
CVE-2022-1690	The Note Press WordPress plugin through 0.1.10 does not sanitise and escape the ids from the bulk actions before using them in a SQL statement in an admin page, leading to an SQL injection	2.7	More Details
CVE-2022-1688	The Note Press WordPress plugin through 0.1.10 does not sanitise and escape the id parameter before using it in various SQL statement via the admin dashboard, leading to SQL Injections	2.7	More Details
CVE-2017-20031	A vulnerability was found in PHPList 3.2.6. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument sortby with the input password leads to information disclosure. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.3.1 is able to address this issue. It is recommended to upgrade the affected component.	2.7	More Details
CVE-2022-2020	A vulnerability, which was classified as problematic, has been found in SourceCodester Prison Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/?page=system_info of the component System Name Handler. The manipulation with the input <img src="" onerror="alert(1)"> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2022-29247	Electron is a framework for writing cross-platform desktop applications using JavaScript (JS), HTML, and CSS. A vulnerability in versions prior to 18.0.0-beta.6, 17.2.0, 16.2.6, and 15.5.5 allows a renderer with JS execution to obtain access to a new renderer process with `nodeIntegrationInSubFrames` enabled which in turn allows effective access to `ipcRenderer`. The `nodeIntegrationInSubFrames` option does not implicitly grant Node.js access. Rather, it depends on the existing sandbox setting. If an application is sandboxed, then `nodeIntegrationInSubFrames` just gives access to the sandboxed renderer APIs, which include `ipcRenderer`. If the application then additionally exposes IPC messages without IPC `senderFrame` validation that perform privileged actions or return confidential data this access to `ipcRenderer` can in turn compromise your application / user even with the sandbox enabled. Electron versions 18.0.0-beta.6, 17.2.0, 16.2.6, and 15.5.5 contain a fix for this issue. As a workaround, ensure that all IPC message handlers appropriately validate `senderFrame`.	2.2	More Details
CVE-2022-2076	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-2021-41454	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-2022-31289	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-2021-41453	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-2022-2077	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-2021-41452	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-2021-46815	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-46789. Reason: This candidate is a duplicate of CVE-2021-46789. Notes: All CVE users should reference CVE-2021-46789 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-41438	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-2021-41439	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-2021-41446	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-2021-41447	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-2021-41448	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