SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 09 March 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-2022-22947	In spring cloud gateway versions prior to 3.1.1+ and 3.0.7+ , applications are vulnerable to a code injection attack when the Gateway Actuator endpoint is enabled, exposed and unsecured. A remote attacker could make a maliciously crafted request that could allow arbitrary remote execution on the remote host.	10.0	More Details
CVE-2022-0767	Server-Side Request Forgery (SSRF) in GitHub repository janeczku/calibre-web prior to 0.6.17.	9.9	More Details
CVE-2021-32008	This issue affects: Secomea GateManager Version 9.6.621421014 and all prior versions. Improper Limitation of a Pathname to restricted directory, allows logged in GateManager admin to delete system Files or Directories.	9.9	More Details
CVE-2022-0845	Code Injection in GitHub repository pytorchlightning/pytorch-lightning prior to 1.6.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24306	Zoho ManageEngine SharePoint Manager Plus before 4329 allows account takeover because authorization is mishandled.	9.8	More Details
CVE-2021-46393	There is a stack buffer overflow vulnerability in the formSetPPTPServer function of Tenda-AX3 router V16.03.12.10_CN. The v10 variable is directly retrieved from the http request parameter startIp. Then v10 will be splice to stack by function sscanf without any security check,which causes stack overflow. By POSTing the page /goform/SetPptpServerCfg with proper startIp, the attacker can easily perform remote code execution with carefully crafted overflow data.	9.8	More Details
CVE-2021-46394	There is a stack buffer overflow vulnerability in the formSetPPTPServer function of Tenda-AX3 router V16.03.12.10_CN. The v13 variable is directly retrieved from the http request parameter startIp. Then v13 will be splice to stack by function sscanf without any security check, which causes stack overflow. By POSTing the page /goform/SetPptpServerCfg with proper startIp, the attacker can easily perform remote code execution with carefully crafted overflow data.	9.8	More Details
CVE-2022-26201	Victor CMS v1.0 was discovered to contain a SQL injection vulnerability.	9.8	More Details
CVE-2022-0839	Improper Restriction of XML External Entity Reference in GitHub repository liquibase/liquibase prior to 4.8.0.	9.8	More Details
CVE-2022-26318	On WatchGuard Firebox and XTM appliances, an unauthenticated user can execute arbitrary code, aka FBX-22786. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2.	9.8	More Details
CVE-2021-46384	https://gitee.com/mingSoft/MCMS MCMS <=5.2.5 is affected by: RCE. The impact is: execute arbitrary code (remote). The attack vector is: ${"freemarker.template.utility.Execute"?new()("calc")}. ¶¶ MCMS has a pre-auth RCE vulnerability through which allows unauthenticated attacker with network access via http to compromise MCMS. Successful attacks of this vulnerability can result in takeover of MCMS.	9.8	More Details
CVE-2022-24305	Zoho ManageEngine SharePoint Manager Plus before 4329 is vulnerable to a sensitive data leak that leads to privilege escalation.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0730	Under certain ldap conditions, Cacti authentication can be bypassed with certain credential types.	9.8	More Details
CVE-2022-26495	In nbd-server in nbd before 3.24, there is an integer overflow with a resultant heap-based buffer overflow. A value of 0xffffffff in the name length field will cause a zero-sized buffer to be allocated for the name, resulting in a write to a dangling pointer. This issue exists for the NBD_OPT_INFO, NBD_OPT_GO, and NBD_OPT_EXPORT_NAME messages.	9.8	More Details
CVE-2022-26496	In nbd-server in nbd before 3.24, there is a stack-based buffer overflow. An attacker can cause a buffer overflow in the parsing of the name field by sending a crafted NBD_OPT_INFO or NBD_OPT_GO message with an large value as the length of the name.	9.8	More Details
CVE-2021-46704	In GenieACS 1.2.x before 1.2.8, the UI interface API is vulnerable to unauthenticated OS command injection via the ping host argument (lib/ui/api.ts and lib/ping.ts). The vulnerability arises from insufficient input validation combined with a missing authorization check.	9.8	More Details
CVE-2022-0766	Server-Side Request Forgery (SSRF) in GitHub repository janeczku/calibre-web prior to 0.6.17.	9.8	More Details
CVE-2022-0349	The NotificationX WordPress plugin before 2.3.9 does not sanitise and escape the nx_id parameter before using it in a SQL statement, leading to an Unauthenticated Blind SQL Injection	9.8	More Details
CVE-2022-0434	The Page View Count WordPress plugin before 2.4.15 does not sanitise and escape the post_ids parameter before using it in a SQL statement via a REST endpoint, available to both unauthenticated and authenticated users. As a result, unauthenticated attackers could perform SQL injection attacks	9.8	More Details
CVE-2022-0441	The MasterStudy LMS WordPress plugin before 2.7.6 does to validate some parameters given when registering a new account, allowing unauthenticated users to register as an admin	9.8	More Details
CVE-2022-26313	A vulnerability has been identified in Mendix Forgot Password Appstore module (All versions >= V3.3.0 < V3.5.1). In certain configurations of the affected product, a threat actor could use the sign up flow to hijack arbitrary user accounts.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46703	In the IsolatedRazorEngine component of Antaris RazorEngine through 4.5.1-alpha001, an attacker can execute arbitrary .NET code in a sandboxed environment (if users can externally control template contents). NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.8	More Details
CVE-2022-0848	OS Command Injection in GitHub repository part-db/part-db prior to 0.5.11.	9.8	More Details
CVE-2022-0265	Improper Restriction of XML External Entity Reference in GitHub repository hazelcast/hazelcast in 5.1-BETA-1.	9.8	More Details
CVE-2021-3762	A directory traversal vulnerability was found in the ClairCore engine of Clair. An attacker can exploit this by supplying a crafted container image which, when scanned by Clair, allows for arbitrary file write on the filesystem, potentially allowing for remote code execution.	9.8	More Details
CVE-2022-25016	Home Owners Collection Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via the component /student_attendance/index.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	9.8	More Details
CVE-2022-23878	seacms V11.5 is affected by an arbitrary code execution vulnerability in admin_config.php.	9.8	More Details
CVE-2022-23640	Excel-Streaming-Reader is an easy-to-use implementation of a streaming Excel reader using Apache POI. Prior to xlsx-streamer 2.1.0, the XML parser that was used did apply all the necessary settings to prevent XML Entity Expansion issues. Upgrade to version 2.1.0 to receive a patch. There is no known workaround.	9.8	More Details
CVE-2022-25045	Home Owners Collection Management System v1.0 was discovered to contain hardcoded credentials which allows attackers to escalate privileges and access the admin panel.	9.8	More Details
CVE-2022-25394	Medical Store Management System v1.0 was discovered to contain a SQL injection vulnerability via the cid parameter under customer-add.php.	9.8	More Details
CVE-2022-25396	Cosmetics and Beauty Product Online Store v1.0 was discovered to contain a SQL injection vulnerability via the search parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25398	Auto Spare Parts Management v1.0 was discovered to contain a SQL injection vulnerability via the user parameter.	9.8	More Details
CVE-2022-25399	Simple Real Estate Portal System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter.	9.8	More Details
CVE-2022-26169	Air Cargo Management System v1.0 was discovered to contain a SQL injection vulnerability via the ref_code parameter.	9.8	More Details
CVE-2022-26170	Simple Mobile Comparison Website v1.0 was discovered to contain a SQL injection vulnerability via the search parameter.	9.8	More Details
CVE-2022-26171	Bank Management System v1.o was discovered to contain a SQL injection vulnerability via the email parameter.	9.8	More Details
CVE-2022-25089	Printix Secure Cloud Print Management through 1.3.1106.0 incorrectly uses Privileged APIs to modify values in HKEY_LOCAL_MACHINE via UITasks.PersistentRegistryData.	9.8	More Details
CVE-2022-0841	OS Command Injection in GitHub repository ljharb/npm-lockfile in v2.0.3 and v2.0.4.	9.8	More Details
CVE-2022-23898	MCMS v5.2.5 was discovered to contain a SQL injection vulnerability via the categoryId parameter in the file IContentDao.xml.	9.8	More Details
CVE-2022-23899	MCMS v5.2.5 was discovered to contain a SQL injection vulnerability via search.do in the file /web/MCmsAction.java.	9.8	More Details
CVE-2022-25125	MCMS v5.2.4 was discovered to contain a SQL injection vulnerability via search.do in the file /mdiy/dict/listExcludeApp.	9.8	More Details
CVE-2022-26314	A vulnerability has been identified in Mendix Forgot Password Appstore module (All versions >= V3.3.0 < V3.5.1), Mendix Forgot Password Appstore module (Mendix 7 compatible) (All versions < V3.2.2). Initial passwords are generated in an insecure manner. This could allow an unauthenticated remote attacker to efficiently brute force passwords in specific situations.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25069	Mark Text v0.16.3 was discovered to contain a DOM-based cross-site scripting (XSS) vulnerability which allows attackers to perform remote code execution (RCE) via injecting a crafted payload into /lib/contentState/pasteCtrl.js.	9.6	More Details
CVE-2022-25395	Cosmetics and Beauty Product Online Store v1.0 was discovered to contain multiple reflected cross-site scripting (XSS) attacks via the search parameter under the /cbpos/ app.	9.6	More Details
CVE-2021-37208	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC, RUGGEDCOM i802, RUGGEDCOM i802NC, RUGGEDCOM i803, RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM M2100F, RUGGEDCOM M2100NC, RUGGEDCOM M2200, RUGGEDCOM M2200F, RUGGEDCOM M2200NC, RUGGEDCOM M969, RUGGEDCOM M969F, RUGGEDCOM M969NC, RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC, RUGGEDCOM RS400, RUGGEDCOM RS400F, RUGGEDCOM RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC, RUGGEDCOM RS416, RUGGEDCOM RS416F, RUGGEDCOM RS416NC, RUGGEDCOM RS416NCv2 V4.X, RUGGEDCOM RS416NCv2 V5.X, RUGGEDCOM RS416P, RUGGEDCOM RS416PF, RUGGEDCOM RS416PNC, RUGGEDCOM RS416PNCv2 V4.X, RUGGEDCOM RS416PNCv2 V5.X, RUGGEDCOM RS416Pv2 V4.X, RUGGEDCOM RS416Pv2 V5.X, RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC, RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900F, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GF, RUGGEDCOM RS900GNC, RUGGEDCOM RS900GNC(32M) V4.X, RUGGEDCOM RS900GNC(32M) V5.X, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPF, RUGGEDCOM RS900GPNC, RUGGEDCOM RS900L, RUGGEDCOM RS900LNC, RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-GETS-XX, RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM RS900MNC-STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM	9.6	More Details

CVE Number	Description	Base Score	Reference
	RS900NC(32M) V4.X, RUGGEDCOM RS900NC(32M) V5.X, RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GF, RUGGEDCOM RS940GNC, RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100F, RUGGEDCOM RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PF, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200F, RUGGEDCOM RSG2200NC, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300F, RUGGEDCOM RSG2300NC V4.X, RUGGEDCOM RSG2300NC V5.X, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PF, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488F, RUGGEDCOM RSG2488NC V4.X, RUGGEDCOM RSG2488NC V5.X, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM RSL910, RUGGEDCOM RSL910NC, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. Improper neutralization of special characters on the web server configuration page could allow an attacker, in a privileged position, to retrieve sensitive information via cross-site scripting.		
CVE-2022-25312	An XML external entity (XXE) injection vulnerability was discovered in the Any23 RDFa XSLTStylesheet extractor and is known to affect Any23 versions < 2.7. XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem, and to interact with any back-end or external systems that the application itself can access. This issue is fixed in Apache Any23 2.7.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2021-44827	There is remote authenticated OS command injection on TP-Link Archer C20i 0.9.1 3.2 v003a.0 Build 170221 Rel.55462n devices vie the X_TP_ExternalIPv6Address HTTP parameter, allowing a remote attacker to run arbitrary commands on the router with root privileges.	8.8	More Details
CVE-2020-18326	Cross Site Request Forgery (CSRF) vulnerability exists in Intelliants Subrion CMS v4.2.1 via the Members administrator function, which could let a remote unauthenticated malicious user send an authorised request to victim and successfully create an arbitrary administrator user.	8.8	More Details
CVE-2022-22909	HotelDruid v3.0.3 was discovered to contain a remote code execution (RCE) vulnerability which is exploited via an attacker inserting a crafted payload into the name field under the Create New Room module.	8.8	More Details
CVE-2021-42950	Remote Code Execution (RCE) vulnerability exists in Zepl Notebooks all previous versions before October 25 2021. Users can register for an account and are allocated a set number of credits to try the product. Once users authenticate, they can proceed to create a new organization by which additional users can be added for various collaboration abilities, which allows malicious user to create new Zepl Notebooks with various languages, contexts, and deployment scenarios. Upon creating a new notebook with specially crafted malicious code, a user can then launch remote code execution.	8.8	More Details
CVE-2021-41001	An authenticated remote code execution vulnerability was discovered in the AOS-CX Network Analytics Engine (NAE) in Aruba CX 6200F Switch Series, Aruba 6300 Switch Series, Aruba 6400 Switch Series, Aruba 8320 Switch Series, Aruba 8325 Switch Series, Aruba 8400 Switch Series, Aruba CX 8360 Switch Series version(s): AOS-CX 10.07.xxxx: 10.07.0050 and below, AOS-CX 10.08.xxxx: 10.08.1030 and below, AOS-CX 10.09.xxxx: 10.09.0002 and below. Aruba has released upgrades for Aruba AOS-CX devices that address this security vulnerability.	8.8	More Details
CVE-2021-41000	Multiple authenticated remote code execution vulnerabilities were discovered in the AOS-CX command line interface in Aruba CX 6200F Switch Series, Aruba 6300 Switch Series, Aruba 6400 Switch Series, Aruba 8320 Switch Series, Aruba 8325 Switch Series, Aruba 8400 Switch Series, Aruba CX 8360 Switch Series version(s): AOS-CX 10.06.xxxx: 10.06.0170 and below, AOS-CX 10.07.xxxx: 10.07.0050 and below, AOS-CX 10.08.xxxx: 10.08.1030 and below. Aruba has released upgrades for Aruba AOS-CX devices that address these security vulnerabilities.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0439	The Email Subscribers & Newsletters WordPress plugin before 5.3.2 does not correctly escape the `order` and `orderby` parameters to the `ajax_fetch_report_list` action, making it vulnerable to blind SQL injection attacks by users with roles as low as Subscriber. Further, it does not have any CSRF protection in place for the action, allowing an attacker to trick any logged in user to perform the action by clicking a link.	8.8	More Details
CVE-2022-0410	The WP Visitor Statistics (Real Time Traffic) WordPress plugin before 5.6 does not sanitise and escape the id parameter before using it in a SQL statement via the refUrlDetails AJAX action, available to any authenticated user, leading to a SQL injection	8.8	More Details
CVE-2022-0819	Code Injection in GitHub repository dolibarr/dolibarr prior to 15.0.1.	8.8	More Details
CVE-2021-24952	The Conversios.io WordPress plugin before 4.6.2 does not sanitise, validate and escape the sync_progressive_data parameter for the tvcajax_product_sync_bantch_wise AJAX action before using it in a SQL statement, allowing any authenticated user to perform SQL injection attacks.	8.8	More Details
CVE-2022-24724	cmark-gfm is GitHub's extended version of the C reference implementation of CommonMark. Prior to versions 0.29.0.gfm.3 and 0.28.3.gfm.21, an integer overflow in cmark-gfm's table row parsing `table.c:row_from_string` may lead to heap memory corruption when parsing tables who's marker rows contain more than UINT16_MAX columns. The impact of this heap corruption ranges from Information Leak to Arbitrary Code Execution depending on how and where `cmark-gfm` is used. If `cmark-gfm` is used for rendering remote user controlled markdown, this vulnerability may lead to Remote Code Execution (RCE) in applications employing affected versions of the `cmark-gfm` library. This vulnerability has been patched in the following cmark-gfm versions 0.29.0.gfm.3 and 0.28.3.gfm.21. A workaround is available. The vulnerability exists in the table markdown extensions of cmark-gfm. Disabling the table extension will prevent this vulnerability from being triggered.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3738	In DCE/RPC it is possible to share the handles (cookies for resource state) between multiple connections via a mechanism called 'association groups'. These handles can reference connections to our sam.ldb database. However while the database was correctly shared, the user credentials state was only pointed at, and when one connection within that association group ended, the database would be left pointing at an invalid 'struct session_info'. The most likely outcome here is a crash, but it is possible that the use-after-free could instead allow different user state to be pointed at and this might allow more privileged access.	8.8	More Details
CVE-2022-0824	Improper Access Control to Remote Code Execution in GitHub repository webmin/webmin prior to 1.990.	8.8	More Details
CVE-2021-3656	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "virt_ext" field, this issue could allow a malicious L1 to disable both VMLOAD/VMSAVE intercepts and VLS (Virtual VMLOAD/VMSAVE) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape.	8.8	More Details
CVE-2022-22351	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged trusted host user to exploit a vulnerability in the nimsh daemon to cause a denial of service in the nimsh daemon on another trusted host. IBM X-Force ID: 220396	8.6	More Details
CVE-2022-24715	Icinga Web 2 is an open source monitoring web interface, framework and command-line interface. Authenticated users, with access to the configuration, can create SSH resource files in unintended directories, leading to the execution of arbitrary code. This issue has been resolved in versions 2.8.6, 2.9.6 and 2.10 of Icinga Web 2. Users unable to upgrade should limit access to the Icinga Web 2 configuration.	8.5	More Details
CVE-2022-24722	VIewComponent is a framework for building view components in Ruby on Rails. Versions prior to 2.31.2 and 2.49.1 contain a cross-site scripting vulnerability that has the potential to impact anyone using translations with the view_component gem. Data received via user input and passed as an interpolation argument to the `translate` method is not properly sanitized before display. Versions 2.31.2 and 2.49.1 have been released and fully mitigate the vulnerability. As a workaround, avoid passing user input to the `translate` function, or sanitize the inputs before passing them.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25471	An Insecure Direct Object Reference (IDOR) vulnerability in OpenEMR 6.0.0 allows any authenticated attacker to access and modify unauthorized areas via a crafted POST request to /modules/zend_modules/public/Installer/register.	8.1	More Details
CVE-2022-24738	Evmos is the Ethereum Virtual Machine (EVM) Hub on the Cosmos Network. In versions of evmos prior to 2.0.1 attackers are able to drain unclaimed funds from user addresses. To do this an attacker must create a new chain which does not enforce signature verification and connects it to the target evmos instance. The attacker can use this joined chain to transfer unclaimed funds. Users are advised to upgrade. There are no known workarounds for this issue.	8.1	More Details
CVE-2021-41002	Multiple authenticated remote path traversal vulnerabilities were discovered in the AOS-CX command line interface in Aruba CX 6200F Switch Series, Aruba 6300 Switch Series, Aruba 6400 Switch Series, Aruba 8320 Switch Series, Aruba 8325 Switch Series, Aruba 8400 Switch Series, Aruba CX 8360 Switch Series version(s): AOS-CX 10.06.xxxx: 10.06.0170 and below, AOS-CX 10.07.xxxx: 10.07.0050 and below, AOS-CX 10.08.xxxx: 10.08.1030 and below, AOS-CX 10.09.xxxx: 10.09.0002 and below. Aruba has released upgrades for Aruba AOS-CX devices that address these security vulnerabilities.	8.1	More Details
CVE-2021-23214	When the server is configured to use trust authentication with a clientcert requirement or to use cert authentication, a man-in-the-middle attacker can inject arbitrary SQL queries when a connection is first established, despite the use of SSL certificate verification and encryption.	8.1	More Details
CVE-2022-0829	Improper Authorization in GitHub repository webmin/webmin prior to 1.990.	8.1	More Details
CVE-2022-0492	A vulnerability was found in the Linux kernel's cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_agent feature to escalate privileges and bypass the namespace isolation unexpectedly.	7.8	More Details
CVE-2021-20319	An improper signature verification vulnerability was found in coreos-installer. A specially crafted gzip installation image can bypass the image signature verification and as a consequence can lead to the installation of unsigned content. An attacker able to modify the original installation image can write arbitrary data, and achieve full access to the node being installed.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23729	When the device is in factory state, it can be access the shell without adb authentication process. The LG ID is LVE-SMP-210010.	7.8	More Details
CVE-2022-25115	A remote code execution (RCE) vulnerability in the Avatar parameter under /admin/?page=user/manage_user of Home Owners Collection Management System v1.0 allows attackers to execute arbitrary code via a crafted PNG file.	7.8	More Details
CVE-2021-44335	David Brackeen ok-file-formats 203defd is vulnerable to Buffer Overflow. When the function of the ok-file-formats project is used, a heap-buffer-overflow occurs in function ok_png_transform_scanline() in "/ok_png.c:533".	7.8	More Details
CVE-2021-44343	David Brackeen ok-file-formats 203defd is vulnerable to Buffer Overflow. When the function of the ok-file-formats project is used, a heap-buffer-overflow occurred in function ok_png_read_data() in "/ok_png.c".	7.8	More Details
CVE-2022-25465	Espruino 2v11 release was discovered to contain a stack buffer overflow via src/jsvar.c in jsvGetNextSibling.	7.8	More Details
CVE-2021-26948	Null pointer dereference in the htmldoc v1.9.11 and before may allow attackers to execute arbitrary code and cause a denial of service via a crafted html file.	7.8	More Details
CVE-2022-25623	The Symantec Management Agent is susceptible to a privilege escalation vulnerability. A low privilege local account can be elevated to the SYSTEM level through registry manipulations.	7.8	More Details
CVE-2021-26259	A flaw was found in htmldoc in v1.9.12. Heap buffer overflow in render_table_row(),in ps-pdf.cxx may lead to arbitrary code execution and denial of service.	7.8	More Details
CVE-2022-22706	Arm Mali GPU Kernel Driver allows a non-privileged user to achieve write access to read-only memory pages. This affects Midgard r26p0 through r31p0, Bifrost r0p0 through r35p0, and Valhall r19p0 through r35p0.	7.8	More Details
CVE-2022-26129	Buffer overflow vulnerabilities exist in FRRouting through 8.1.0 due to wrong checks on the subtlv length in the functions, parse_hello_subtlv, parse_ihu_subtlv, and parse_update_subtlv in babeld/message.c.	7.8	More Details
CVE-2022-25031	Remote Desktop Commander Suite Agent before v4.8 contains an unquoted service path which allows attackers to escalate privileges to the system level.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26125	Buffer overflow vulnerabilities exist in FRRouting through 8.1.0 due to wrong checks on the input packet length in isisd/isis_tlvs.c.	7.8	More Details
CVE-2022-25044	Espruino 2v11.251 was discovered to contain a stack buffer overflow via src/jsvar.c in jsvNewFromString.	7.8	More Details
CVE-2021-3575	A heap-based buffer overflow was found in openjpeg in color.c:379:42 in sycc420_to_rgb when decompressing a crafted .j2k file. An attacker could use this to execute arbitrary code with the permissions of the application compiled against openjpeg.	7.8	More Details
CVE-2021-4199	Incorrect Permission Assignment for Critical Resource vulnerability in the crash handling component BDReinit.exe as used in Bitdefender Total Security, Internet Security, Antivirus Plus, Endpoint Security Tools for Windows allows a remote attacker to escalate local privileges to SYSTEM. This issue affects: Bitdefender Total Security versions prior to 26.0.10.45. Bitdefender Internet Security versions prior to 26.0.10.45. Bitdefender Antivirus Plus versions prior to 26.0.10.45. Bitdefender Endpoint Security Tools for Windows versions prior to 7.4.3.146.	7.8	More Details
CVE-2021-3715	A flaw was found in the "Routing decision" classifier in the Linux kernel's Traffic Control networking subsystem in the way it handled changing of classification filters, leading to a use-after-free condition. This flaw allows unprivileged local users to escalate their privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	7.8	More Details
CVE-2022-26127	A buffer overflow vulnerability exists in FRRouting through 8.1.0 due to missing a check on the input packet length in the babel_packet_examin function in babeld/message.c.	7.8	More Details
CVE-2022-26128	A buffer overflow vulnerability exists in FRRouting through 8.1.0 due to a wrong check on the input packet length in the babel_packet_examin function in babeld/message.c.	7.8	More Details
CVE-2022-26490	st21nfca_connectivity_event_received in drivers/nfc/st21nfca/se.c in the Linux kernel through 5.16.12 has EVT_TRANSACTION buffer overflows because of untrusted length parameters.	7.8	More Details
CVE-2022-26337	Trend Micro Password Manager (Consumer) installer version 5.0.0.1262 and below is vulnerable to an Uncontrolled Search Path Element vulnerability that could allow an attacker to use a specially crafted file to exploit the vulnerability and escalate local privileges on the affected machine.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26126	Buffer overflow vulnerabilities exist in FRRouting through 8.1.0 due to the use of strdup with a non-zero-terminated binary string in isis_nb_notifications.c.	7.8	More Details
CVE-2022-24661	A vulnerability has been identified in Simcenter STAR-CCM+ Viewer (All versions < V2022.1). The starview+.exe contains a memory corruption vulnerability while parsing specially crafted .SCE files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2022-22301	An improper neutralization of special elements used in an OS Command vulnerability [CWE-78] in FortiAP-C console 5.4.0 through 5.4.3, 5.2.0 through 5.2.1 may allow an authenticated attacker to execute unauthorized commands by running CLI commands with specifically crafted arguments.	7.8	More Details
CVE-2021-23180	A flaw was found in htmldoc in v1.9.12 and before. Null pointer dereference in file_extension(),in file.c may lead to execute arbitrary code and denial of service.	7.8	More Details
CVE-2021-23206	A flaw was found in htmldoc in v1.9.12 and prior. A stack buffer overflow in parse_table() in ps-pdf.cxx may lead to execute arbitrary code and denial of service.	7.8	More Details
CVE-2021-23191	A security issue was found in htmldoc v1.9.12 and before. A NULL pointer dereference in the function image_load_jpeg() in image.cxx may result in denial of service.	7.8	More Details
CVE-2022-24408	A vulnerability has been identified in SINUMERIK MC (All versions < V1.15 SP1), SINUMERIK ONE (All versions < V6.15 SP1). The sc SUID binary on affected devices provides several commands that are used to execute system commands or modify system files. A specific set of operations using sc could allow local attackers to escalate their privileges to root.	7.8	More Details
CVE-2022-0711	A flaw was found in the way HAProxy processed HTTP responses containing the "Set-Cookie2" header. This flaw could allow an attacker to send crafted HTTP response packets which lead to an infinite loop, eventually resulting in a denial of service condition. The highest threat from this vulnerability is availability.	7.5	More Details
CVE-2022-25634	Qt through 5.15.8 and 6.x through 6.2.3 can load system library files from an unintended working directory.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23327	A design flaw in Go-Ethereum 1.10.12 and older versions allows an attacker node to send 5120 future transactions with a high gas price in one message, which can purge all of pending transactions in a victim node's memory pool, causing a denial of service (DoS).	7.5	More Details
CVE-2021-23192	A flaw was found in the way samba implemented DCE/RPC. If a client to a Samba server sent a very large DCE/RPC request, and chose to fragment it, an attacker could replace later fragments with their own data, bypassing the signature requirements.	7.5	More Details
CVE-2022-23648	containerd is a container runtime available as a daemon for Linux and Windows. A bug was found in containerd prior to versions 1.6.1, 1.5.10, and 1.14.12 where containers launched through containerd's CRI implementation on Linux with a specially-crafted image configuration could gain access to read-only copies of arbitrary files and directories on the host. This may bypass any policy-based enforcement on container setup (including a Kubernetes Pod Security Policy) and expose potentially sensitive information. Kubernetes and crictl can both be configured to use containerd's CRI implementation. This bug has been fixed in containerd 1.6.1, 1.5.10, and 1.4.12. Users should update to these versions to resolve the issue.	7.5	More Details
CVE-2021-40636	OS4ED openSIS 8.0 is affected by SQL Injection in CheckDuplicateName.php, which can extract information from the database.	7.5	More Details
CVE-2021-25087	The Download Manager WordPress plugin before 3.2.35 does not have any authorisation checks in some of the REST API endpoints, allowing unauthenticated attackers to call them, which could lead to sensitive information disclosure, such as posts passwords (fixed in 3.2.24) and files Master Keys (fixed in 3.2.25).	7.5	More Details
CVE-2021-40635	OS4ED openSIS 8.0 is affected by SQL injection in ChooseCpSearch.php, ChooseRequestSearch.php. An attacker can inject a SQL query to extract information from the database.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42016	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i801, RUGGEDCOM i802, RUGGEDCOM i803, RUGGEDCOM M2100, RUGGEDCOM M2100F, RUGGEDCOM M2200, RUGGEDCOM M2200F, RUGGEDCOM M969, RUGGEDCOM M969F, RUGGEDCOM RMC30, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RP110, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600T, RUGGEDCOM RS400, RUGGEDCOM RS400F, RUGGEDCOM RS401, RUGGEDCOM RS416, RUGGEDCOM RS416F, RUGGEDCOM RS416P, RUGGEDCOM RS416PF, RUGGEDCOM RS416Pv2 V4.X, RUGGEDCOM RS416Pv2 V5.X, RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000H, RUGGEDCOM RS8000T, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900F, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GF, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPF, RUGGEDCOM RS900L, RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM RS910L, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GF, RUGGEDCOM RS969, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100F, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PF, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200F, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300F, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PF, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488F, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSL910, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. A timing attack, in a third-party component, could make the retrieval of the private key possible, used for encryption of sensitive data. If a threat actor were to exploit this, the data integrity and security could be compromised.	7.5	More Details
CVE-2021-46378	DLink DIR850 ET850-1.08TRb03 is affected by an incorrect access control vulnerability through an unauthenticated remote configuration download.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42020	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC, RUGGEDCOM i802, RUGGEDCOM i802NC, RUGGEDCOM i803, RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM M2100NC, RUGGEDCOM M2200, RUGGEDCOM M2200NC, RUGGEDCOM M969, RUGGEDCOM M969NC, RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC, RUGGEDCOM RS400, RUGGEDCOM RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC, RUGGEDCOM RS416, RUGGEDCOM RS416NC, RUGGEDCOM RS416NCv2 V4.X, RUGGEDCOM RS416NCv2 V5.X, RUGGEDCOM RS416P, RUGGEDCOM RS416PNC, RUGGEDCOM RS416PNCv2 V4.X, RUGGEDCOM RS416PNCv2 V5.X, RUGGEDCOM RS416Pv2 V4.X, RUGGEDCOM RS416Pv2 V5.X, RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC, RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GNC, RUGGEDCOM RS900GNC(32M) V4.X, RUGGEDCOM RS900GNC(32M) V5.X, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPNC, RUGGEDCOM RS900L, RUGGEDCOM RS900LNC, RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-GETS-XX, RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM RS900MNC-STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM RS900NC(32M) V4.X, RUGGEDCOM RS900NC(32M) V5.X, RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GNC, RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM RSG2100, RUGGEDCOM	7.5	More Details

CVE Number	Description	Base Score	Reference
	RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200NC, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300NC V4.X, RUGGEDCOM RSG2300NC V5.X, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488NC V4.X, RUGGEDCOM RSG2488NC V5.X, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM RSL910, RUGGEDCOM RSL910NC, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. The third-party component, in its TFTP functionality fails to check for null terminations in file names. If an attacker were to exploit this, it could result in data corruption, and possibly a hard-fault of the application.		
CVE-2022-23328	A design flaw in all versions of Go-Ethereum allows an attacker node to send 5120 pending transactions of a high gas price from one account that all fully spend the full balance of the account to a victim Geth node, which can purge all of pending transactions in a victim node's memory pool and then occupy the memory pool to prevent new transactions from entering the pool, resulting in a denial of service (DoS).	7.5	More Details
CVE-2021-46381	Local File Inclusion due to path traversal in D-Link DAP-1620 leads to unauthorized internal files reading [/etc/passwd] and [/etc/shadow].	7.5	More Details
CVE-2021-4076	A flaw exists in tang, a network-based cryptographic binding server, which could result in leak of private keys.	7.5	More Details
CVE-2022-23233	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.6.0 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS) of the Local Distribution Router (LDR) service.	7.5	More Details
CVE-2021-40846	An issue was discovered in Rhinode Trading Paints through 2.0.36. TP Updater.exe uses cleartext HTTP to check, and request, updates. Thus, attackers can man-in-the-middle a victim to download a malicious binary in place of the real update, with no SSL errors or warnings.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27756	"TLS-RSA cipher suites are not disabled in BigFix Compliance up to v2.0.5. If TLS 2.0 and secure ciphers are not enabled then an attacker can passively record traffic and later decrypt it."	7.5	More Details
CVE-2022-24921	regexp.Compile in Go before 1.16.15 and 1.17.x before 1.17.8 allows stack exhaustion via a deeply nested expression.	7.5	More Details
CVE-2021-3737	A flaw was found in python. An improperly handled HTTP response in the HTTP client code of python may allow a remote attacker, who controls the HTTP server, to make the client script enter an infinite loop, consuming CPU time. The highest threat from this vulnerability is to system availability.	7.5	More Details
CVE-2021-38266	The Portal Security module in Liferay Portal 7.2.1 and earlier, and Liferay DXP 7.0 before fix pack 90, 7.1 before fix pack 17 and 7.2 before fix pack 5 does not correctly import users from LDAP, which allows remote attackers to prevent a legitimate user from authenticating by attempting to sign in as a user that exist in LDAP.	7.5	More Details
CVE-2022-24713	regex is an implementation of regular expressions for the Rust language. The regex crate features built-in mitigations to prevent denial of service attacks caused by untrusted regexes, or untrusted input matched by trusted regexes. Those (tunable) mitigations already provide sane defaults to prevent attacks. This guarantee is documented and it's considered part of the crate's API. Unfortunately a bug was discovered in the mitigations designed to prevent untrusted regexes to take an arbitrary amount of time during parsing, and it's possible to craft regexes that bypass such mitigations. This makes it possible to perform denial of service attacks by sending specially crafted regexes to services accepting user-controlled, untrusted regexes. All versions of the regex crate before or equal to 1.5.4 are affected by this issue. The fix is include starting from regex 1.5.5. All users accepting user-controlled regexes are recommended to upgrade immediately to the latest version of the regex crate. Unfortunately there is no fixed set of problematic regexes, as there are practically infinite regexes that could be crafted to exploit this vulnerability. Because of this, it us not recommend to deny known problematic regexes.	7.5	More Details
CVE-2021-27757	" Insecure password storage issue.The application stores sensitive information in cleartext within a resource that might be accessible to another control sphere.Since the information is stored in cleartext, attackers could potentially read it and gain access to sensitive information."	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21716	Twisted is an event-based framework for internet applications, supporting Python 3.6+. Prior to 22.2.0, Twisted SSH client and server implement is able to accept an infinite amount of data for the peer's SSH version identifier. This ends up with a buffer using all the available memory. The attach is a simple as `nc -rv localhost 22 < /dev/zero`. A patch is available in version 22.2.0. There are currently no known workarounds.	7.5	More Details
CVE-2022-25393	Simple Bakery Shop Management v1.0 was discovered to contain a SQL injection vulnerability via the username parameter.	7.5	More Details
CVE-2022-24716	Icinga Web 2 is an open source monitoring web interface, framework and command-line interface. Unauthenticated users can leak the contents of files of the local system accessible to the web-server user, including `icingaweb2` configuration files with database credentials. This issue has been resolved in versions 2.9.6 and 2.10 of Icinga Web 2. Database credentials should be rotated.	7.5	More Details
CVE-2022-26505	A DNS rebinding issue in ReadyMedia (formerly MiniDLNA) before 1.3.1 allows a remote web server to exfiltrate media files.	7.4	More Details
CVE-2021-38578	Existing CommBuffer checks in SmmEntryPoint will not catch underflow when computing BufferSize.	7.4	More Details
CVE-2022-25311	A vulnerability has been identified in SINEC NMS (All versions >= V1.0.3 < V2.0), SINEC NMS (All versions < V1.0.3), SINEMA Server V14 (All versions). The affected software do not properly check privileges between users during the same web browser session, creating an unintended sphere of control. This could allow an authenticated low privileged user to achieve privilege escalation.	7.3	More Details
CVE-2022-24739	alltube is an html front end for youtube-dl. On releases prior to 3.0.3, an attacker could craft a special HTML page to trigger either an open redirect attack or a Server-Side Request Forgery attack (depending on how AllTube is configured). The impact is mitigated by the fact the SSRF attack is only possible when the `stream` option is enabled in the configuration. (This option is disabled by default.) 3.0.3 contains a fix for this vulnerability.	7.3	More Details
CVE-2021-24778	The test parameter of the xmlfeed in the Tradetracker-Store WordPress plugin before 4.6.60 is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24777	The view submission functionality in the Hotscot Contact Form WordPress plugin before 1.3 makes a get request with the sub_id parameter which not sanitised, escaped or validated before inserting to a SQL statement, leading to an SQL injection.	7.2	More Details
CVE-2022-23915	The package weblate from 0 and before 4.11.1 are vulnerable to Remote Code Execution (RCE) via argument injection when using git or mercurial repositories. Authenticated users, can change the behavior of the application in an unintended way, leading to command execution.	7.2	More Details
CVE-2021-24216	The All-in-One WP Migration WordPress plugin before 7.41 does not validate uploaded files' extension, which allows administrators to upload PHP files on their site, even on multisite installations.	7.2	More Details
CVE-2022-0420	The RegistrationMagic WordPress plugin before 5.0.2.2 does not sanitise and escape the rm_form_id parameter before using it in a SQL statement in the Automation admin dashboard, allowing high privilege users to perform SQL injection attacks	7.2	More Details
CVE-2022-24282	A vulnerability has been identified in SINEC NMS (All versions >= V1.0.3 < V2.0), SINEC NMS (All versions < V1.0.3), SINEMA Server V14 (All versions). The affected system allows to upload JSON objects that are deserialized to Java objects. Due to insecure deserialization of user-supplied content by the affected software, a privileged attacker could exploit this vulnerability by sending a maliciously crafted serialized Java object. This could allow the attacker to execute arbitrary code on the device with root privileges.	7.2	More Details
CVE-2022-0440	The Catch Themes Demo Import WordPress plugin before 2.1.1 does not validate one of the file to be imported, which could allow high privivilege admin to upload an arbitrary PHP file and gain RCE even in the case of an hardened blog (ie DISALLOW_UNFILTERED_HTML, DISALLOW_FILE_EDIT and DISALLOW_FILE_MODS constants set to true)	7.2	More Details
CVE-2022-21828	A user with high privilege access to the Incapptic Connect web console can remotely execute code on the Incapptic Connect server using a unspecified attack vector in Incapptic Connect version 1.40.0, 1.39.1, 1.39.0, 1.38.1, 1.38.0, 1.37.1, 1.37.0, 1.36.0, 1.35.5, 1.35.4 and 1.35.3.	7.2	More Details
CVE-2022-0267	The AdRotate WordPress plugin before 5.8.22 does not sanitise and escape the adrotate_action before using it in a SQL statement via the adrotate_request_action function available to admins, leading to a SQL injection	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24281	A vulnerability has been identified in SINEC NMS (All versions < V1.0.3), SINEMA Server V14 (All versions). A privileged authenticated attacker could execute arbitrary commands in the local database by sending specially crafted requests to the webserver of the affected application.	7.2	More Details
CVE-2021-43944	This issue exists to document that a security improvement in the way that Jira Server and Data Center use templates has been implemented. Affected versions of Atlassian Jira Server and Data Center allowed remote attackers with system administrator permissions to execute arbitrary code via Template Injection leading to Remote Code Execution (RCE) in the Email Templates feature. The affected versions are before version 8.13.15, and from version 8.14.0 before 8.20.3.	7.2	More Details
CVE-2021-3743	An out-of-bounds (OOB) memory read flaw was found in the Qualcomm IPC router protocol in the Linux kernel. A missing sanity check allows a local attacker to gain access to out-of-bounds memory, leading to a system crash or a leak of internal kernel information. The highest threat from this vulnerability is to system availability.	7.1	More Details
CVE-2021-3609	.A flaw was found in the CAN BCM networking protocol in the Linux kernel, where a local attacker can abuse a flaw in the CAN subsystem to corrupt memory, crash the system or escalate privileges. This race condition in net/can/bcm.c in the Linux kernel allows for local privilege escalation to root.	7.0	More Details
CVE-2021-3640	A flaw use-after-free in function sco_sock_sendmsg() of the Linux kernel HCI subsystem was found in the way user calls ioct UFFDIO_REGISTER or other way triggers race condition of the call sco_conn_del() together with the call sco_sock_sendmsg() with the expected controllable faulting memory page. A privileged local user could use this flaw to crash the system or escalate their privileges on the system.	7.0	More Details
CVE-2022-24309	A vulnerability has been identified in Mendix Runtime V7 (All versions < V7.23.29), Mendix Runtime V8 (All versions < V8.18.16), Mendix Runtime V9 (All versions < V9.13 only with Runtime Custom Setting *DataStorage.UseNewQueryHandler* set to False). If an entity has an association readable by the user, then in some cases, Mendix Runtime may not apply checks for XPath constraints that parse said associations, within apps running on affected versions. A malicious user could use this to dump and manipulate sensitive data.	6.8	More Details
	A vulnerability has been identified in RUGGEDCOM i800 (All versions < V4.3.8), RUGGEDCOM i801 (All versions < V4.3.8), RUGGEDCOM i802 (All versions < V4.3.8), RUGGEDCOM i803 (All versions < V4.3.8), RUGGEDCOM M2100 (All versions < V4.3.8), RUGGEDCOM M2200 (All versions < V4.3.8), RUGGEDCOM M969 (All versions < V4.3.8),		

CVE Number	Description	Base Score	Reference
	RUGGEDCOM RMC30 (All versions < V4.3.8), RUGGEDCOM RMC8388 V4.X (All versions < V4.3.8), RUGGEDCOM RMC8388 V5.X (All versions < V5.7.0), RUGGEDCOM RP110 (All versions < V4.3.8), RUGGEDCOM		
CVE-2021-37209	RS1600 (All versions < V4.3.8), RUGGEDCOM RS1600F (All versions < V4.3.8), RUGGEDCOM RS1600T (All versions < V4.3.8), RUGGEDCOM RS400 (All versions < V4.3.8), RUGGEDCOM RS401 (All versions < V4.3.8), RUGGEDCOM RS416 (All versions < V4.3.8), RUGGEDCOM RS416P (All versions < V4.3.8), RUGGEDCOM RS416Pv2 V4.X (All versions < V4.3.8), RUGGEDCOM RS416Pv2 V5.X (All versions < V5.7.0), RUGGEDCOM RS416v2 V4.X (All versions < V4.3.8), RUGGEDCOM RS416v2 V5.X (All versions < V5.7.0), RUGGEDCOM RS8000 (All versions < V4.3.8), RUGGEDCOM RS8000A (All versions < V4.3.8), RUGGEDCOM RS8000H (All versions < V4.3.8), RUGGEDCOM RS8000T (All versions < V4.3.8), RUGGEDCOM RS900 (All versions < V4.3.8), RUGGEDCOM RS900 (32M) V4.X (All versions < V4.3.8), RUGGEDCOM RS900 (32M) V5.X (All versions < V5.7.0), RUGGEDCOM RS900G (All versions < V4.3.8), RUGGEDCOM RS900G (32M) V4.X (All versions < V4.3.8), RUGGEDCOM RS900G (32M) V5.X (All versions < V5.7.0), RUGGEDCOM RS900GP (All versions < V4.3.8), RUGGEDCOM RS900L (All versions < V4.3.8), RUGGEDCOM RS900M-GETS-C01 (All versions < V4.3.8), RUGGEDCOM RS900M-GETS-XX (All versions < V4.3.8), RUGGEDCOM RS900M-STND-C01 (All versions < V4.3.8), RUGGEDCOM RS900M-STND-XX (All versions < V4.3.8), RUGGEDCOM RS900W (All versions < V4.3.8), RUGGEDCOM RS910 (All versions < V4.3.8), RUGGEDCOM RS910L (All versions < V4.3.8), RUGGEDCOM RS910W (All versions < V4.3.8), RUGGEDCOM RS920L (All versions < V4.3.8), RUGGEDCOM RS920W (All versions < V4.3.8), RUGGEDCOM RS930L (All versions < V4.3.8), RUGGEDCOM RS930W (All versions < V4.3.8), RUGGEDCOM RS940G (All versions < V4.3.8), RUGGEDCOM RS969 (All versions < V4.3.8), RUGGEDCOM RSG2100 (All versions < V4.3.8), RUGGEDCOM RSG2100 (32M) V4.X (All versions < V4.3.8), RUGGEDCOM RSG2100 (32M) V5.X (All versions < V5.7.0), RUGGEDCOM RSG2100P (All versions < V4.3.8), RUGGEDCOM RSG2200 (All versions < V4.3.8), RUGGEDCOM RSG2288 V4.X (All versions < V4.3.8), RUGGEDCOM RSG2288 V5.X (All versions < V5.7.0), RUGGEDCOM RSG2300 V4.X (All versions < V4.3.8), RUGGEDCOM RSG2300 V5.X (All versions < V5.7.0), RUGGEDCOM RSG2300P V4.X (All versions < V4.3.8), RUGGEDCOM RSG2300P V5.X (All versions < V5.7.0), RUGGEDCOM RSG2488 V4.X (All versions < V4.3.8), RUGGEDCOM RSG2488 V5.X (All versions < V5.7.0), RUGGEDCOM RSG907R (All versions < V5.7.0), RUGGEDCOM RSG908C (All versions < V5.7.0), RUGGEDCOM RSG909R (All versions < V5.7.0), RUGGEDCOM RSG910C (All versions < V5.7.0), RUGGEDCOM RSG920P V4.X (All versions < V4.3.8), RUGGEDCOM RSG920P V5.X (All versions < V5.7.0), RUGGEDCOM RSL910 (All versions < V5.7.0), RUGGEDCOM RST2228 (All versions < V5.7.0), RUGGEDCOM RST2228P (All versions < V5.7.0), RUGGEDCOM RST916C (All versions < V5.7.0), RUGGEDCOM RST916P (All versions	6.7	More Details

CVE Number	Description	Base Score	Reference
	< V5.7.0). The SSH server on affected devices is configured to offer weak ciphers by default. This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over the connection between legitimate clients and the affected device.		
CVE-2022-22943	VMware Tools for Windows (11.x.y and 10.x.y prior to 12.0.0) contains an uncontrolled search path vulnerability. A malicious actor with local administrative privileges in the Windows guest OS, where VMware Tools is installed, may be able to execute code with system privileges in the Windows guest OS due to an uncontrolled search path element.	6.7	More Details
CVE-2022-23849	The biometric lock in Devolutions Password Hub for iOS before 2021.3.4 allows attackers to access the application because of authentication bypass. An attacker must rapidly make failed biometric authentication attempts.	6.6	More Details
CVE-2021-3677	A flaw was found in postgresql. A purpose-crafted query can read arbitrary bytes of server memory. In the default configuration, any authenticated database user can complete this attack at will. The attack does not require the ability to create objects. If server settings include max_worker_processes=0, the known versions of this attack are infeasible. However, undiscovered variants of the attack may be independent of that setting.	6.5	More Details
CVE-2021-3772	A flaw was found in the Linux SCTP stack. A blind attacker may be able to kill an existing SCTP association through invalid chunks if the attacker knows the IP-addresses and port numbers being used and the attacker can send packets with spoofed IP addresses.	6.5	More Details
CVE-2022-0577	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository scrapy/scrapy prior to 2.6.1.	6.5	More Details
CVE-2022-26319	An installer search patch element vulnerability in Trend Micro Portable Security 3.0 Pro, 3.0 and 2.0 could allow a local attacker to place an arbitrarily generated DLL file in an installer folder to elevate local privileges. Please note: an attacker must first obtain the ability to execute high-privileged code on the target system in order to exploit this vulnerability.	6.5	More Details
CVE-2022-23052	PeteReport Version 0.5 contains a Cross Site Request Forgery (CSRF) vulnerability allowing an attacker to trick users into deleting users, products, reports and findings on the application.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26317	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.29). When returning the result of a completed Microflow execution call the affected framework does not correctly verify, if the request was initially made by the user requesting the result. Together with predictable identifiers for Microflow execution calls, this could allow a malicious attacker to retrieve information about arbitrary Microflow execution calls made by users within the affected system.	6.5	More Details
CVE-2022-24737	HTTPie is a command-line HTTP client. HTTPie has the practical concept of sessions, which help users to persistently store some of the state that belongs to the outgoing requests and incoming responses on the disk for further usage. Before 3.1.0, HTTPie didn‘t distinguish between cookies and hosts they belonged. This behavior resulted in the exposure of some cookies when there are redirects originating from the actual host to a third party website. Users are advised to upgrade. There are no known workarounds.	6.5	More Details
CVE-2021-41543	A vulnerability has been identified in Climatix POL909 (AWB module) (All versions < V11.44), Climatix POL909 (AWM module) (All versions < V11.36). The handling of log files in the web application of affected devices contains an information disclosure vulnerability which could allow logged in users to access sensitive files.	6.5	More Details
CVE-2021-3667	An improper locking issue was found in the virStoragePoolLookupByTargetPath API of libvirt. It occurs in the storagePoolLookupByTargetPath function where a locked virStoragePoolObj object is not properly released on ACL permission failure. Clients connecting to the read-write socket with limited ACL permissions could use this flaw to acquire the lock and prevent other users from accessing storage pool/volume APIs, resulting in a denial of service condition. The highest threat from this vulnerability is to system availability.	6.5	More Details
CVE-2022-0756	Missing Authorization in GitHub repository salesagility/suitecrm prior to 7.12.5.	6.5	More Details
CVE-2022-24447	An issue was discovered in Zoho ManageEngine Key Manager Plus before 6200. A service exposed by the application allows a user, with the level Operator, to access stored SSL certificates and associated key pairs during export.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3658	bluetoothd from bluez incorrectly saves adapters' Discoverable status when a device is powered down, and restores it when powered up. If a device is powered down while discoverable, it will be discoverable when powered on again. This could lead to inadvertent exposure of the bluetooth stack to physically nearby attackers.	6.5	More Details
CVE-2021-3638	An out-of-bounds memory access flaw was found in the ATI VGA device emulation of QEMU. This flaw occurs in the ati_2d_blt() routine while handling MMIO write operations when the guest provides invalid values for the destination display parameters. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service.	6.5	More Details
CVE-2022-0528	Server-Side Request Forgery (SSRF) in GitHub repository transloadit/uppy prior to 3.3.1.	6.5	More Details
CVE-2022-0163	The Smart Forms WordPress plugin before 2.6.71 does not have authorisation in its rednao_smart_forms_entries_list AJAX action, allowing any authenticated users, such as subscriber, to download arbitrary form's data, which could include sensitive information such as PII depending on the form.	6.5	More Details
CVE-2022-0754	SQL Injection in GitHub repository salesagility/suitecrm prior to 7.12.5.	6.5	More Details
CVE-2022-0445	The WordPress Real Cookie Banner: GDPR (DSGVO) & ePrivacy Cookie Consent WordPress plugin before 2.14.2 does not have CSRF checks in place when resetting its settings, allowing attackers to make a logged in admin reset them via a CSRF attack	6.5	More Details
CVE-2021-38268	The Dynamic Data Mapping module in Liferay Portal 7.0.0 through 7.3.6, and Liferay DXP 7.0 before fix pack 101, 7.1 before fix pack 21, 7.2 before fix pack 10 and 7.3 before fix pack 2 incorrectly sets default permissions for site members, which allows remote authenticated users with the site member role to add and duplicate forms, via the UI or the API.	6.5	More Details
CVE-2021-25098	The Pricing Tables WordPress Plugin WordPress plugin before 3.1.3 does not verify the CSRF nonce when removing posts, allowing attackers to make a logged in admin remove arbitrary posts from the blog via a CSRF attack, which will be put in the trash	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45819	Wordline HIDCCEMonitorSVC before v5.2.4.3 contains an unquoted service path which allows attackers to escalate privileges to the system level.	6.4	More Details
CVE-2021-3631	A flaw was found in libvirt while it generates SELinux MCS category pairs for VMs' dynamic labels. This flaw allows one exploited guest to access files labeled for another guest, resulting in the breaking out of sVirt confinement. The highest threat from this vulnerability is to confidentiality and integrity.	6.3	More Details
CVE-2021-43392	STMicroelectronics STSAFE-J 1.1.4, J-SAFE3 1.2.5, and J-SIGN sometimes allow attackers to obtain information on cryptographic secrets. This is associated with the ECDSA signature algorithm on the Java Card J-SAFE3 and STSAFE-J platforms exposing a 3.0.4 Java Card API. It is exploitable for STSAFE-J in closed configuration and J-SIGN (when signature verification is activated) but not for J-SAFE3 EPASS BAC and EAC products. It might also impact other products based on the J-SAFE-3 Java Card platform.	6.2	More Details
CVE-2021-43393	STMicroelectronics STSAFE-J 1.1.4, J-SAFE3 1.2.5, and J-SIGN sometimes allow attackers to abuse signature verification. This is associated with the ECDSA signature algorithm on the Java Card J-SAFE3 and STSAFE-J platforms exposing a 3.0.4 Java Card API. It is exploitable for STSAFE-J in closed configuration and J-SIGN (when signature verification is activated) but not for J-SAFE3 EPASS BAC and EAC products. It might also impact other products based on the J-SAFE-3 Java Card platform.	6.2	More Details
CVE-2022-24725	Shescape is a shell escape package for JavaScript. An issue in versions 1.4.0 to 1.5.1 allows for exposure of the home directory on Unix systems when using Bash with the `escape` or `escapeAll` functions from the _shescape_ API with the `interpolation` option set to `true`. Other tested shells, Dash and Zsh, are not affected. Depending on how the output of _shescape_ is used, directory traversal may be possible in the application using _shescape_. The issue was patched in version 1.5.1. As a workaround, manually escape all instances of the tilde character (`~`) using `arg.replace(/~/g, "\\~")`.	6.2	More Details
CVE-2021-20303	A flaw found in function dataWindowForTile() of IlmImf/ImfTiledMisc.cpp. An attacker who is able to submit a crafted file to be processed by OpenEXR could trigger an integer overflow, leading to an out-of-bounds write on the heap. The greatest impact of this flaw is to application availability, with some potential impact to data integrity as well.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46382	Unauthenticated cross-site scripting (XSS) in Netgear WAC120 AC Access Point may lead to mulitple attacks like session hijacking even clipboard hijacking.	6.1	More Details
CVE-2022-0697	Open Redirect in GitHub repository archivy/archivy prior to 1.7.0.	6.1	More Details
CVE-2022-0429	The WP Cerber Security, Anti-spam & Malware Scan WordPress plugin before 8.9.6 does not sanitise the $url variable before using it in an attribute in the Activity tab in the plugins dashboard, leading to an unauthenticated stored Cross-Site Scripting vulnerability.	6.1	More Details
CVE-2021-36809	A local attacker can overwrite arbitrary files on the system with VPN client logs using administrator privileges, potentially resulting in a denial of service and data loss, in all versions of Sophos SSL VPN client.	6.1	More Details
CVE-2021-44478	A vulnerability has been identified in Polarion ALM (All versions < V21 R2 P2), Polarion WebClient for SVN (All versions). A cross-site scripting is present due to improper neutralization of data sent to the web page through the SVN WebClient in the affected product. An attacker could exploit this to execute arbitrary code and extract sensitive information by sending a specially crafted link to users with administrator privileges.	6.1	More Details
CVE-2022-0868	Open Redirect in GitHub repository medialize/uri.js prior to 1.19.10.	6.1	More Details
CVE-2022-0869	Multiple Open Redirect in GitHub repository nitely/spirit prior to 0.12.3.	6.1	More Details
CVE-2022-0855	Improper Resolution of Path Equivalence in GitHub repository microweber-dev/whmcs_plugin prior to 0.0.4.	6.1	More Details
CVE-2021-41541	A vulnerability has been identified in Climatix POL909 (AWB module) (All versions < V11.44), Climatix POL909 (AWM module) (All versions < V11.36). The Group Management page of affected devices is vulnerable to cross-site scripting (XSS). The vulnerability allows an attacker to send malicious JavaScript code which could result in hijacking of the user's cookie/session tokens, redirecting the user to a malicious webpage and performing unintended browser action.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38264	Cross-site scripting (XSS) vulnerability in the Frontend Taglib module in Liferay Portal 7.4.0 and 7.4.1 allows remote attackers to inject arbitrary web script or HTML into the management toolbar search via the `keywords` parameter. This issue is caused by an incomplete fix in CVE-2021-35463.	6.1	More Details
CVE-2022-0533	The Ditty (formerly Ditty News Ticker) WordPress plugin before 3.0.15 is affected by a Reflected Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-38263	Cross-site scripting (XSS) vulnerability in the Server module's script console in Liferay Portal 7.3.2 and earlier, and Liferay DXP 7.0 before fix pack 101, 7.1 before fix pack 20 and 7.2 before fix pack 10 allows remote attackers to inject arbitrary web script or HTML via the output of a script.	6.1	More Details
CVE-2021-25039	The WordPress Multisite Content Copier/Updater WordPress plugin before 2.1.0 does not sanitise and escape the wmcc_content_type, wmcc_source_blog and wmcc_record_per_page parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting issues	6.1	More Details
CVE-2021-3623	A flaw was found in libtpms. The flaw can be triggered by specially-crafted TPM 2 command packets containing illegal values and may lead to an out-of-bounds access when the volatile state of the TPM 2 is marshalled/written or unmarshalled/read. The highest threat from this vulnerability is to system availability.	6.1	More Details
CVE-2022-25114	Event Management v1.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the full_name parameter under register.php.	6.1	More Details
CVE-2021-4198	A NULL Pointer Dereference vulnerability in the messaging_ipc.dll component as used in Bitdefender Total Security, Internet Security, Antivirus Plus, Endpoint Security Tools, VPN Standalone allows an attacker to arbitrarily crash product processes and generate crashdump files. This issue affects: Bitdefender Total Security versions prior to 26.0.3.29. Bitdefender Internet Security versions prior to 26.0.3.29. Bitdefender Antivirus Plus versions prior to 26.0.3.29. Bitdefender Endpoint Security Tools versions prior to 7.2.2.92. Bitdefender VPN Standalone versions prior to 25.5.0.48.	6.1	More Details
CVE-2022-0422	The White Label CMS WordPress plugin before 2.2.9 does not sanitise and validate the wlcms[_login_custom_js] parameter before outputting it back in the response while previewing, leading to a Reflected Cross-Site Scripting issue	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0753	Cross-site Scripting (XSS) - Reflected in GitHub repository hestiacp/hestiacp prior to 1.5.9.	6.1	More Details
CVE-2021-46379	DLink DIR850 ET850-1.08TRb03 is affected by an incorrect access control vulnerability through URL redirection to untrusted site.	6.1	More Details
CVE-2020-18325	Multilple Cross Site Scripting (XSS) vulnerability exists in Intelliants Subrion CMS v4.2.1 in the Configuration panel.	6.1	More Details
CVE-2022-23710	A cross-site-scripting (XSS) vulnerability was discovered in the Data Preview Pane (previously known as Index Pattern Preview Pane) which could allow arbitrary JavaScript to be executed in a victim’s browser.	6.1	More Details
CVE-2021-25038	The WordPress Multisite User Sync/Unsync WordPress plugin before 2.1.2 does not sanitise and escape the wmus_source_blog and wmus_record_per_page parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting issues	6.1	More Details
CVE-2022-0838	Cross-site Scripting (XSS) - Reflected in GitHub repository hestiacp/hestiacp prior to 1.5.10.	6.1	More Details
CVE-2022-0752	Cross-site Scripting (XSS) - Generic in GitHub repository hestiacp/hestiacp prior to 1.5.9.	6.1	More Details
CVE-2021-40637	OS4ED openSIS 8.0 is affected by cross-site scripting (XSS) in EmailCheckOthers.php. An attacker can inject JavaScript code to get the user's cookie and take over the working session of user.	6.1	More Details
CVE-2021-41003	Multiple unauthenticated command injection vulnerabilities were discovered in the AOS-CX API interface in Aruba CX 6200F Switch Series, Aruba 6300 Switch Series, Aruba 6400 Switch Series, Aruba 8320 Switch Series, Aruba 8325 Switch Series, Aruba 8400 Switch Series, Aruba CX 8360 Switch Series version(s): AOS-CX 10.06.xxxx: 10.06.0170 and below, AOS-CX 10.07.xxxx: 10.07.0050 and below, AOS-CX 10.08.xxxx: 10.08.1030 and below, AOS-CX 10.09.xxxx: 10.09.0002 and below. Aruba has released upgrades for Aruba AOS-CX devices that address these security vulnerabilities.	6.1	More Details
CVE-2021-3654	A vulnerability was found in openstack-nova's console proxy, noVNC. By crafting a malicious URL, noVNC could be made to redirect to any desired URL.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-18324	Cross Site Scripting (XSS) vulnerability exists in Subrion CMS 4.2.1 via the q parameter in the Kickstart template.	6.1	More Details
CVE-2021-24953	The Advanced iFrame WordPress plugin before 2022 does not sanitise and escape the ai_config_id parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2022-0347	The LoginPress	Custom Login Page Customizer WordPress plugin before 1.5.12 does not escape the redirect-page parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-23397	The Cedar Gate EZ-NET portal 6.5.5 6.8.0 Internet portal has a call to display messages to users which does not properly sanitize data sent in through a URL parameter. This leads to a Reflected Cross-Site Scripting vulnerability. NOTE: the vendor disputes this because the ado.im reference has "no clear steps of reproduction."	6.1	More Details
CVE-2022-23395	jQuery Cookie 1.4.1 is affected by prototype pollution, which can lead to DOM cross-site scripting (XSS).	6.1	More Details
CVE-2020-18327	Cross Site Scripting (XSS) vulnerability exists in Alfresco Alfresco Community Edition v5.2.0 via the action parameter in the alfresco/s/admin/admin-nodebrowser API. Fixed in v6.2	6.1	More Details
CVE-2021-41542	A vulnerability has been identified in Climatix POL909 (AWB module) (All versions < V11.44), Climatix POL909 (AWM module) (All versions < V11.36). The User Management page of affected devices is vulnerable to cross-site scripting (XSS). The vulnerability allows an attacker to send malicious JavaScript code which could result in hijacking of the user's cookie/session tokens, redirecting the user to a malicious webpage and performing unintended browser action.	6.1	More Details
CVE-2022-24573	A stored cross-site scripting (XSS) vulnerability in the admin interface in Element-IT HTTP Commander 7.0.0 allows unauthenticated users to get admin access by injecting a malicious script in the User-Agent field.	6.1	More Details
CVE-2021-43590	Dell EMC Enterprise Storage Analytics for vRealize Operations, versions 4.0.1 to 6.2.1, contain a Plain-text password storage vulnerability. A local high privileged malicious user may potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23222	A man-in-the-middle attacker can inject false responses to the client's first few queries, despite the use of SSL certificate verification and encryption.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42017	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i801, RUGGEDCOM i802, RUGGEDCOM i803, RUGGEDCOM M2100, RUGGEDCOM M2100F, RUGGEDCOM M2200, RUGGEDCOM M2200F, RUGGEDCOM M969, RUGGEDCOM M969F, RUGGEDCOM RMC30, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RP110, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600T, RUGGEDCOM RS400, RUGGEDCOM RS400F, RUGGEDCOM RS401, RUGGEDCOM RS416, RUGGEDCOM RS416F, RUGGEDCOM RS416P, RUGGEDCOM RS416PF, RUGGEDCOM RS416Pv2 V4.X, RUGGEDCOM RS416Pv2 V5.X, RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000H, RUGGEDCOM RS8000T, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900F, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GF, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPF, RUGGEDCOM RS900L, RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM RS910L, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GF, RUGGEDCOM RS969, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100F, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PF, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200F, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300F, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PF, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488F, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSL910, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. A new variant of the POODLE attack has left a third-party component vulnerable due to the implementation flaws of the CBC encryption mode in TLS 1.0 to 1.2. If an attacker were to exploit this, they could act as a man-in-the-middle and eavesdrop on encrypted communications.	5.9	More Details
	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC, RUGGEDCOM		

CVE Number	Description	Base Score	Reference
	i802, RUGGEDCOM i802NC, RUGGEDCOM i803, RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM M2100F, RUGGEDCOM M2100NC, RUGGEDCOM M2200, RUGGEDCOM M2200F,		
CVE-2021-42018	RUGGEDCOM M2200NC, RUGGEDCOM M969, RUGGEDCOM M969F, RUGGEDCOM M969NC, RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC, RUGGEDCOM RS400, RUGGEDCOM RS400F, RUGGEDCOM RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC, RUGGEDCOM RS416, RUGGEDCOM RS416F, RUGGEDCOM RS416NC, RUGGEDCOM RS416NCv2 V4.X, RUGGEDCOM RS416NCv2 V5.X, RUGGEDCOM RS416P, RUGGEDCOM RS416PF, RUGGEDCOM RS416PNC, RUGGEDCOM RS416PNCv2 V4.X, RUGGEDCOM RS416PNCv2 V5.X, RUGGEDCOM RS416Pv2 V4.X, RUGGEDCOM RS416Pv2 V5.X, RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC, RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900F, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GF, RUGGEDCOM RS900GNC, RUGGEDCOM RS900GNC(32M) V4.X, RUGGEDCOM RS900GNC(32M) V5.X, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPF, RUGGEDCOM RS900GPNC, RUGGEDCOM RS900L, RUGGEDCOM RS900LNC, RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-GETS-XX, RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM RS900MNC-STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM RS900NC(32M) V4.X, RUGGEDCOM RS900NC(32M) V5.X, RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GF, RUGGEDCOM RS940GNC, RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100F, RUGGEDCOM RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PF, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200F, RUGGEDCOM RSG2200NC, RUGGEDCOM	5.9	More Details

CVE Number	Description	Base Score	Reference
	RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300F, RUGGEDCOM RSG2300NC V4.X, RUGGEDCOM RSG2300NC V5.X, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PF, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488F, RUGGEDCOM RSG2488NC V4.X, RUGGEDCOM RSG2488NC V5.X, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM RSL910, RUGGEDCOM RSL910NC, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. Within a third-party component, whenever memory allocation is requested, the out of bound size is not checked. Therefore, if size exceeding the expected allocation is assigned, it could allocate a smaller buffer instead. If an attacker were to exploit this, they could cause a heap overflow.		
	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC, RUGGEDCOM i802, RUGGEDCOM i802NC, RUGGEDCOM i803, RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM M2100F, RUGGEDCOM M2100NC, RUGGEDCOM M2200, RUGGEDCOM M2200F, RUGGEDCOM M2200NC, RUGGEDCOM M969, RUGGEDCOM M969F, RUGGEDCOM M969NC, RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC, RUGGEDCOM RS400, RUGGEDCOM RS400F, RUGGEDCOM RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC, RUGGEDCOM RS416, RUGGEDCOM RS416F, RUGGEDCOM RS416NC, RUGGEDCOM RS416NCv2 V4.X, RUGGEDCOM RS416NCv2 V5.X, RUGGEDCOM RS416P, RUGGEDCOM RS416PF, RUGGEDCOM RS416PNC, RUGGEDCOM RS416PNCv2 V4.X, RUGGEDCOM RS416PNCv2 V5.X, RUGGEDCOM RS416Pv2 V4.X, RUGGEDCOM RS416Pv2 V5.X, RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC, RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900F, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GF, RUGGEDCOM RS900GNC, RUGGEDCOM		

CVE Number	Description	Base Score	Reference
	RS900GNC(32M) V4.X, RUGGEDCOM RS900GNC(32M) V5.X, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPF, RUGGEDCOM RS900GPNC, RUGGEDCOM RS900L, RUGGEDCOM RS900LNC,		
CVE-2021-42019	RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-GETS-XX, RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM RS900MNC-STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM RS900NC(32M) V4.X, RUGGEDCOM RS900NC(32M) V5.X, RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GF, RUGGEDCOM RS940GNC, RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100F, RUGGEDCOM RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PF, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200F, RUGGEDCOM RSG2200NC, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300F, RUGGEDCOM RSG2300NC V4.X, RUGGEDCOM RSG2300NC V5.X, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PF, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488F, RUGGEDCOM RSG2488NC V4.X, RUGGEDCOM RSG2488NC V5.X, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM RSL910, RUGGEDCOM RSL910NC, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. Within a third-party component, the process to allocate partition size fails to check memory boundaries. Therefore, if a large amount is requested by an attacker, due to an integer-wrap around, it could result in a small size being allocated instead.	5.9	More Details
CVE-2022-0675	In certain situations it is possible for an unmanaged rule to exist on the target system that has the same comment as the rule specified in the manifest. This could allow for unmanaged rules to exist on the target system and leave the system in an unsafe state.	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44748	A vulnerability affecting F-Secure SAFE browser was discovered whereby browsers loads images automatically this vulnerability can be exploited remotely by an attacker to execute the JavaScript can be used to trigger universal cross-site scripting through the browser. User interaction is required prior to exploitation, such as entering a malicious website to trigger the vulnerability.	5.5	More Details
CVE-2022-0849	Use After Free in r_reg_get_name_idx in GitHub repository radareorg/radare2 prior to 5.6.6.	5.5	More Details
CVE-2021-38989	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX kernel to cause a denial of service. IBM X-Force ID: 212951.	5.5	More Details
CVE-2021-38988	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX kernel to cause a denial of service. IBM X-Force ID: 212950.	5.5	More Details
CVE-2021-44749	A vulnerability affecting F-Secure SAFE browser protection was discovered improper URL handling can be triggered to cause universal cross-site scripting through browsing protection in a SAFE web browser. User interaction is required prior to exploitation. A successful exploitation may lead to arbitrary code execution.	5.5	More Details
CVE-2021-45860	An integer overflow in DTSStreamReader::findFrame() of tsMuxer git-2678966 allows attackers to cause a Denial of Service (DoS) via a crafted file.	5.5	More Details
CVE-2022-25106	D-Link DIR-859 v1.05 was discovered to contain a stack-based buffer overflow via the function genacgi_main. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload.	5.5	More Details
CVE-2021-3602	An information disclosure flaw was found in Buildah, when building containers using chroot isolation. Running processes in container builds (e.g. Dockerfile RUN commands) can access environment variables from parent and grandparent processes. When run in a container in a CI/CD environment, environment variables may include sensitive information that was shared with the container in order to be used only by Buildah itself (e.g. container registry credentials).	5.5	More Details
CVE-2022-23956	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23953	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service.	5.5	More Details
CVE-2022-23955	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service.	5.5	More Details
CVE-2022-22350	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in CAA to cause a denial of service. IBM X-Force ID: 220394.	5.5	More Details
CVE-2022-23957	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service.	5.5	More Details
CVE-2022-23958	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service.	5.5	More Details
CVE-2021-38996	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX kernel to cause a denial of service. IBM X-Force ID: 213076.	5.5	More Details
CVE-2022-23954	Potential vulnerabilities have been identified in the BIOS for some HP PC products which may allow denial of service.	5.5	More Details
CVE-2021-3744	A memory leak flaw was found in the Linux kernel in the ccp_run_aes_gcm_cmd() function in drivers/crypto/ccp/ccp-ops.c, which allows attackers to cause a denial of service (memory consumption). This vulnerability is similar with the older CVE-2019-18808.	5.5	More Details
CVE-2021-45861	There is an Assertion `num <= INT_BIT' failed at BitStreamReader::skipBits in /bitStream.h:132 of tsMuxer git-c6a0277.	5.5	More Details
CVE-2022-22946	In spring cloud gateway versions prior to 3.1.1+ , applications that are configured to enable HTTP2 and no key store or trusted certificates are set will be configured to use an insecure TrustManager. This makes the gateway able to connect to remote services with invalid or custom certificates.	5.5	More Details
CVE-2021-20302	A flaw was found in OpenEXR's TiledInputFile functionality. This flaw allows an attacker who can submit a crafted single-part non-image to be processed by OpenEXR, to trigger a floating-point exception error. The highest threat from this vulnerability is to system availability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3620	A flaw was found in Ansible Engine's ansible-connection module, where sensitive information such as the Ansible user credentials is disclosed by default in the traceback error message. The highest threat from this vulnerability is to confidentiality.	5.5	More Details
CVE-2021-45863	tsMuxer git-2678966 was discovered to contain a heap-based buffer overflow via the function HevcUnit::updateBits in hevc.cpp.	5.5	More Details
CVE-2021-45864	tsMuxer git-c6a0277 was discovered to contain a segmentation fault via DTSStreamReader::findFrame in dtsStreamReader.cpp.	5.5	More Details
CVE-2022-25050	rtl_433 21.12 was discovered to contain a stack overflow in the function somfy_iohc_decode(). This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted file.	5.5	More Details
CVE-2021-20300	A flaw was found in OpenEXR's hufUncompress functionality in OpenEXR/IlmImf/ImfHuf.cpp. This flaw allows an attacker who can submit a crafted file that is processed by OpenEXR, to trigger an integer overflow. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2022-25051	An Off-by-one Error occurs in cmr113_decode of rtl_433 21.12 when decoding a crafted file.	5.5	More Details
CVE-2022-26336	A shortcoming in the HMEF package of poi-scratchpad (Apache POI) allows an attacker to cause an Out of Memory exception. This package is used to read TNEF files (Microsoft Outlook and Microsoft Exchange Server). If an application uses poi-scratchpad to parse TNEF files and the application allows untrusted users to supply them, then a carefully crafted file can cause an Out of Memory exception. This issue affects poi-scratchpad version 5.2.0 and prior versions. Users are recommended to upgrade to poi-scratchpad 5.2.1.	5.5	More Details
CVE-2021-3428	A flaw was found in the Linux kernel. A denial of service problem is identified if an extent tree is corrupted in a crafted ext4 filesystem in fs/ext4/extents.c in ext4_es_cache_extent. Fabricating an integer overflow, A local attacker with a special user privilege may cause a system crash problem which can lead to an availability threat.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38267	Cross-site scripting (XSS) vulnerability in the Blogs module's edit blog entry page in Liferay Portal 7.3.2 through 7.3.6, and Liferay DXP 7.3 before fix pack 2 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_blogs_web_portlet_BlogsAdminPortlet_title and _com_liferay_blogs_web_portlet_BlogsAdminPortlet_subtitle parameter.	5.4	More Details
CVE-2021-38265	Cross-site scripting (XSS) vulnerability in the Asset module in Liferay Portal 7.3.4 through 7.3.6 allow remote attackers to inject arbitrary web script or HTML when creating a collection page via the _com_liferay_asset_list_web_portlet_AssetListPortlet_title parameter.	5.4	More Details
CVE-2021-38269	Cross-site scripting (XSS) vulnerability in the Gogo Shell module in Liferay Portal 7.1.0 through 7.3.6 and 7.4.0, and Liferay DXP 7.1 before fix pack 23, 7.2 before fix pack 13, and 7.3 before fix pack 2 allows remote attackers to inject arbitrary web script or HTML via the output of a Gogo Shell command.	5.4	More Details
CVE-2022-0426	The Product Feed PRO for WooCommerce WordPress plugin before 11.2.3 does not escape the rowCount parameter before outputting it back in an attribute via the woosea_categories_dropdown AJAX action (available to any authenticated user), leading to a Reflected Cross-Site Scripting	5.4	More Details
CVE-2022-24563	In Genixcms v1.1.11, a stored Cross-Site Scripting (XSS) vulnerability exists in /gxadmin/index.php?page=themes&view=options" via the intro_title and intro_image parameters.	5.4	More Details
CVE-2022-25138	Axelor Open Suite v5.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Name parameter.	5.4	More Details
CVE-2022-0205	The YOP Poll WordPress plugin before 6.3.5 does not sanitise and escape some of the settings (available to users with a role as low as author) before outputting them, leading to a Stored Cross-Site Scripting issue	5.4	More Details
CVE-2022-0832	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.3.3.	5.4	More Details
CVE-2022-23051	PeteReport Version 0.5 allows an authenticated admin user to inject persistent JavaScript code while adding an 'Attack Tree' by modifying the 'svg_file' parameter.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22944	VMware Workspace ONE Boxer contains a stored cross-site scripting (XSS) vulnerability. Due to insufficient sanitization and validation, in VMware Workspace ONE Boxer calendar event descriptions, a malicious actor can inject script tags to execute arbitrary script within a user's window.	5.4	More Details
CVE-2021-24961	The WordPress File Upload WordPress plugin before 4.16.3, wordpress-file-upload-pro WordPress plugin before 4.16.3 does not escape some of its shortcode argument, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks	5.4	More Details
CVE-2021-43070	Multiple relative path traversal vulnerabilities [CWE-23] in FortiWLM management interface 8.6.2 and below, 8.5.2 and below, 8.4.2 and below, 8.3.3 and below, 8.2.2 may allow an authenticated attacker to retrieve arbitrary files from the underlying filesystem via specially crafted web requests.	5.4	More Details
CVE-2022-0831	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.3.3.	5.4	More Details
CVE-2021-24826	The Custom Content Shortcode WordPress plugin before 4.0.2 does not escape custom fields before outputting them, which could allow Contributor+ (v < 4.0.1) or Admin+ (v < 4.0.2) users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed. Please note that such attack is still possible by admin+ in single site blogs by default (but won't be when the unfiltered_html is disallowed)	5.4	More Details
CVE-2021-24821	The Cost Calculator WordPress plugin before 1.6 allows users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks via the Description fields of a Cost Calculator > Price Settings (which gets injected on the edit page as well as any page that embeds the calculator using the shortcode), as well as the Text Preview field of a Project (injected on the edit project page)	5.4	More Details
CVE-2022-0877	Cross-site Scripting (XSS) - Stored in GitHub repository bookstackapp/bookstack prior to v22.02.3.	5.4	More Details
CVE-2021-24960	The WordPress File Upload WordPress plugin before 4.16.3, wordpress-file-upload-pro WordPress plugin before 4.16.3 allows users with a role as low as Contributor to configure the upload form in a way that allows uploading of SVG files, which could be then be used for Cross-Site Scripting attacks	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24723	URI.js is a Javascript URL mutation library. Before version 1.19.9, whitespace characters are not removed from the beginning of the protocol, so URLs are not parsed properly. This issue has been patched in version 1.19.9. Removing leading whitespace from values before passing them to URI.parse can be used as a workaround.	5.3	More Details
CVE-2022-25146	The Remote App module in Liferay Portal Liferay Portal v7.4.3.4 through v7.4.3.8 and Liferay DXP 7.4 before update 5 does not check if the origin of event messages it receives matches the origin of the Remote App, allowing attackers to exfiltrate the CSRF token via a crafted event message.	5.3	More Details
CVE-2022-23779	Zoho ManageEngine Desktop Central before 10.1.2137.8 exposes the installed server name to anyone. The internal hostname can be discovered by reading HTTP redirect responses.	5.3	More Details
CVE-2021-41239	Nextcloud server is a self hosted system designed to provide cloud style services. In affected versions the User Status API did not consider the user enumeration settings by the administrator. This allowed a user to enumerate other users on the instance, even when user listings where disabled. It is recommended that the Nextcloud Server is upgraded to 20.0.14, 21.0.6 or 22.2.1. There are no known workarounds.	5.3	More Details
CVE-2022-24714	Icinga Web 2 is an open source monitoring web interface, framework and command-line interface. Installations of Icinga 2 with the IDO writer enabled are affected. If you use service custom variables in role restrictions, and you regularly decommission service objects, users with said roles may still have access to a collection of content. Note that this only applies if a role has implicitly permitted access to hosts, due to permitted access to at least one of their services. If access to a host is permitted by other means, no sensible information has been disclosed to unauthorized users. This issue has been resolved in versions 2.8.6, 2.9.6 and 2.10 of Icinga Web 2.	5.3	More Details
CVE-2022-22700	CyberArk Identity versions up to and including 22.1 in the 'StartAuthentication' resource, exposes the response header 'X-CFY-TX-TM'. In certain configurations, that response header contains different, predictable value ranges which can be used to determine whether a user exists in the tenant.	5.3	More Details
CVE-2021-46353	An information disclosure in web interface in D-Link DIR-X1860 before 1.03 RevA1 allows a remote unauthenticated attacker to send a specially crafted HTTP request and gain knowledge of different absolute paths that are being used by the web application.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25009	The CorreosExpress WordPress plugin through 2.6.0 generates log files which are publicly accessible, and contain sensitive information such as sender/receiver names, phone numbers, physical and email addresses	5.3	More Details
CVE-2021-44321	Mini-Inventory-and-Sales-Management-System is affected by Cross Site Request Forgery (CSRF), where an attacker can update/delete items in the inventory. The attacker must be logged into the application create a malicious file for updating the inventory details and items.	5.0	More Details
CVE-2022-26484	An issue was discovered in Veritas InfoScale Operations Manager (VIOM) before 7.4.2 Patch 600 and 8.x before 8.0.0 Patch 100. The web server fails to sanitize admin/cgi-bin/rulemgr.pl/getfile/ input data, allowing a remote authenticated administrator to read arbitrary files on the system via Directory Traversal. By manipulating the resource name in GET requests referring to files with absolute paths, it is possible to access arbitrary files stored on the filesystem, including application source code, configuration files, and critical system files.	4.9	More Details
CVE-2022-23232	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.6.0 are susceptible to a vulnerability which when successfully exploited could allow disabled, expired, or locked external user accounts to access S3 data to which they previously had access. StorageGRID 11.6.0 obtains the user account status from Active Directory or Azure and will block S3 access for disabled user accounts during the subsequent background synchronization. User accounts that are expired or locked for Active Directory or Azure, or user accounts that are disabled, expired, or locked in identity sources other than Active Directory or Azure must be manually removed from group memberships or have their S3 keys manually removed from Tenant Manager in all versions of StorageGRID (formerly StorageGRID Webscale).	4.9	More Details
CVE-2021-43774	A risky-algorithm issue was discovered on Fujifilm DocuCentre-VI C4471 1.8 devices. An attacker that obtained access to the administrative web interface of a printer (e.g., by using the default credentials) can download the address book file, which contains the list of users (domain users, FTP users, etc.) stored on the printer, together with their encrypted passwords. The passwords are protected by a weak cipher, such as ROT13, which requires minimal effort to instantly retrieve the original password, giving the attacker a list of valid domain or FTP usernames and passwords.	4.9	More Details
CVE-2022-0535	The E2Pdf WordPress plugin before 1.16.45 does not sanitise and escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0389	The WP Time Slots Booking Form WordPress plugin before 1.1.63 does not sanitise and escape Calendar names, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-26483	An issue was discovered in Veritas InfoScale Operations Manager (VIOM) before 7.4.2 Patch 600 and 8.x before 8.0.0 Patch 100. A reflected cross-site scripting (XSS) vulnerability in admin/cgi-bin/listdir.pl allows authenticated remote administrators to inject arbitrary web script or HTML into an HTTP GET parameter (which reflect the user input without sanitization).	4.8	More Details
CVE-2021-24810	The WP Event Manager WordPress plugin before 3.1.23 does not escape some of its Field Editor settings when outputting them, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-25220	PeteReport Version 0.5 allows an authenticated admin user to inject persistent JavaScript code inside the markdown descriptions while creating a product, report or finding.	4.8	More Details
CVE-2022-0448	The CP Blocks WordPress plugin before 1.0.15 does not sanitise and escape its "License ID" settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.	4.8	More Details
CVE-2021-41180	Nextcloud talk is a self hosting messaging service. In versions prior 12.1.2 an attacker is able to control the link of a geolocation preview in the Nextcloud Talk application due to a lack of validation on the link. This could result in an open-redirect, but required user interaction. This only affected users of the Android Talk client. It is recommended that the Nextcloud Talk App is upgraded to 12.1.2. There are no known workarounds.	4.7	More Details
CVE-2022-23656	Zulip is an open source team chat app. The `main` development branch of Zulip Server from June 2021 and later is vulnerable to a cross-site scripting vulnerability on the recent topics page. An attacker could maliciously craft a full name for their account and send messages to a topic with several participants; a victim who then opens an overflow tooltip including this full name on the recent topics page could trigger execution of JavaScript code controlled by the attacker. Users running a Zulip server from the main branch should upgrade from main (2022-03-01 or later) again to deploy this fix.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4002	A memory leak flaw in the Linux kernel's hugetlbfs memory usage was found in the way the user maps some regions of memory twice using shmget() which are aligned to PUD alignment with the fault of some of the memory pages. A local user could use this flaw to get unauthorized access to some data.	4.4	More Details
CVE-2022-23708	A flaw was discovered in Elasticsearch 7.17.0’s upgrade assistant, in which upgrading from version 6.x to 7.x would disable the in-built protections on the security index, allowing authenticated users with “*” index permissions access to this index.	4.3	More Details
CVE-2022-0755	Missing Authorization in GitHub repository salesagility/suitecrm prior to 7.12.5.	4.3	More Details
CVE-2022-0442	The UsersWP WordPress plugin before 1.2.3.1 is missing access controls when updating a user avatar, and does not make sure file names for user avatars are unique, allowing a logged in user to overwrite another users avatar.	4.3	More Details
CVE-2021-24824	The [field] shortcode included with the Custom Content Shortcode WordPress plugin before 4.0.1, allows authenticated users with a role as low as contributor, to access arbitrary post metadata. This could lead to sensitive data disclosure, for example when used in combination with WooCommerce, the email address of orders can be retrieved	4.3	More Details
CVE-2021-24825	The Custom Content Shortcode WordPress plugin before 4.0.2 does not validate the data passed to its load shortcode, which could allow Contributor+ (v < 4.0.1) or Admin+ (v < 4.0.2) users to display arbitrary files from the filesystem (such as logs, .htaccess etc), as well as perform Local File Inclusion attacks as PHP files will be executed. Please note that such attack is still possible by admin+ in single site blogs by default (but won't be when either the unfiltered_html or file_edit is disallowed)	4.3	More Details
CVE-2021-41241	Nextcloud server is a self hosted system designed to provide cloud style services. The groupfolders application for Nextcloud allows sharing a folder with a group of people. In addition, it allows setting "advanced permissions" on subfolders, for example, a user could be granted access to the groupfolder but not specific subfolders. Due to a lacking permission check in affected versions, a user could still access these subfolders by copying the groupfolder to another location. It is recommended that the Nextcloud Server is upgraded to 20.0.14, 21.0.6 or 22.2.1. Users unable to upgrade should disable the "groupfolders" application in the admin settings.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23709	A flaw was discovered in Kibana in which users with Read access to the Uptime feature could modify alerting rules. A user with this privilege would be able to create new alerting rules or overwrite existing ones. However, any new or modified rules would not be enabled, and a user with this privilege could not modify alerting connectors. This effectively means that Read users could disable existing alerting rules.	4.3	More Details
CVE-2021-45074	JFrog Artifactory before 7.29.3 and 6.23.38, is vulnerable to Broken Access Control, a low-privileged user is able to delete other known users OAuth token, which will force a reauthentication on an active session or in the next UI session.	4.3	More Details
CVE-2022-0384	The Video Conferencing with Zoom WordPress plugin before 3.8.17 does not have authorisation in its vczapi_get_wp_users AJAX action, allowing any authenticated users, such as subscriber to download the list of email addresses registered on the blog	4.3	More Details
CVE-2021-44166	An improper access control vulnerability [CWE-284] in FortiToken Mobile (Android) external push notification 5.1.0 and below may allow a remote attacker having already obtained a user's password to access the protected system during the 2FA procedure, even though the deny button is clicked by the legitimate user.	4.1	More Details
CVE-2021-3716	A flaw was found in nbdkit due to to improperly caching plaintext state across the STARTTLS encryption boundary. A MitM attacker could use this flaw to inject a plaintext NBD_OPT_STRUCTURED_REPLY before proxying everything else a client sends to the server, potentially leading the client to terminate the NBD session. The highest threat from this vulnerability is to system availability.	3.1	More Details
CVE-2022-22303	An exposure of sensitive system information to an unauthorized control sphere vulnerability [CWE-497] in FortiManager versions prior to 7.0.2, 6.4.7 and 6.2.9 may allow a low privileged authenticated user to gain access to the FortiGate users credentials via the config conflict file.	2.8	More Details
CVE-2021-46270	JFrog Artifactory before 7.31.10, is vulnerable to Broken Access Control where a project admin user is able to list all available repository names due to insufficient permission validation.	2.7	More Details
CVE-2021-41181	Nextcloud talk is a self hosting messaging service. In versions prior to 12.3.0 the Nextcloud Android Talk application did not properly detect the lockscreen state when a call was incoming. If an attacker got physical access to the locked phone, and the victim received a phone call the attacker could gain access to the chat messages and files of the user. It is recommended that the Nextcloud Android Talk App is upgraded to 12.3.0. There are no known workarounds.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46380	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: Reason: This is a duplicate to CVE-2022-22511 Notes	N/A	More Details
CVE-2022-24727	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-23915. Reason: This candidate is a reservation duplicate of CVE-2022-23915. Notes: All CVE users should reference CVE-2022-23915 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-26487	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-26143. Reason: This candidate is a reservation duplicate of CVE-2022-26143. Notes: All CVE users should reference CVE-2022-26143 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-22688	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-22687	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-22693	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-22694	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-22690	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22691	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-22686	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-38577	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This CVE has been rejected as it was incorrectly assigned. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2021-22695	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-22692	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-22689	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details