SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 30 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-2021-27470	A deserialization vulnerability exists in how the LogService.rem service in Rockwell Automation FactoryTalk AssetCentre v10.00 and earlier verifies serialized data. This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary commands in FactoryTalk AssetCentre.	10.0	More Details
CVE-2021-27462	A deserialization vulnerability exists in how the AosService.rem service in Rockwell Automation FactoryTalk AssetCentre v10.00 and earlier verifies serialized data. This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary commands in FactoryTalk AssetCentre.	10.0	More Details
CVE-2021-27476	A vulnerability exists in the SaveConfigFile function of the RACompare Service, which may allow for OS command injection. This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary commands in Rockwell Automation FactoryTalk AssetCentre v10.00 and earlier.	10.0	More Details
CVE-2021-27474	Rockwell Automation FactoryTalk AssetCentre v10.00 and earlier does not properly restrict all functions relating to IIS remoting services. This vulnerability may allow a remote, unauthenticated attacker to modify sensitive data in FactoryTalk AssetCentre.	10.0	More Details
CVE-2021-27472	A vulnerability exists in the RunSearch function of SearchService service in Rockwell Automation FactoryTalk AssetCentre v10.00 and earlier, which may allow for the execution of remote unauthenticated arbitrary SQL statements.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27468	The AosService.rem service in Rockwell Automation FactoryTalk AssetCentre v10.00 and earlier exposes functions lacking proper authentication. This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary SQL statements.	10.0	More Details
CVE-2021-27466	A deserialization vulnerability exists in how the ArchiveService.rem service in Rockwell Automation FactoryTalk AssetCentre v10.00 and earlier verifies serialized data. This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary commands in FactoryTalk AssetCentre.	10.0	More Details
CVE-2021-27464	The ArchiveService.rem service in Rockwell Automation FactoryTalk AssetCentre v10.00 and earlier exposes functions lacking proper authentication. This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary SQL statements.	10.0	More Details
CVE-2021-27460	Rockwell Automation FactoryTalk AssetCentre v10.00 and earlier components contain .NET remoting endpoints that deserialize untrusted data without sufficiently verifying that the resulting data will be valid. This vulnerability may allow a remote, unauthenticated attacker to gain full access to the FactoryTalk AssetCentre main server and all agent machines.	10.0	More Details
CVE-2022-24783	Deno is a runtime for JavaScript and TypeScript. The versions of Deno between release 1.18.0 and 1.20.2 (inclusive) are vulnerable to an attack where a malicious actor controlling the code executed in a Deno runtime could bypass all permission checks and execute arbitrary shell code. This vulnerability does not affect users of Deno Deploy. The vulnerability has been patched in Deno 1.20.3. There is no workaround. All users are recommended to upgrade to 1.20.3 immediately.	10.0	More Details
CVE-2021-46433	In fenom 2.12.1 and before, there is a way in fenom/src/Fenom/Template.php function getTemplateCode()to bypass sandbox to execute arbitrary PHP code when disable_native_funcs is true.	10.0	More Details
CVE-2022-22995	The combination of primitives offered by SMB and AFP in their default configuration allows the arbitrary writing of files. By exploiting these combination of primitives, an attacker can execute arbitrary code.	10.0	More Details
CVE-2022-0735	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.10 before 14.6.5, all versions starting from 14.7 before 14.7.4, all versions starting from 14.8 before 14.8.2. An unauthorised user was able to steal runner registration tokens through an information disclosure vulnerability using quick actions commands.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24768	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All unpatched versions of Argo CD starting with 1.0.0 are vulnerable to an improper access control bug, allowing a malicious user to potentially escalate their privileges to admin-level. Versions starting with 0.8.0 and 0.5.0 contain limited versions of this issue. To perform exploits, an authorized Argo CD user must have push access to an Application's source git or Helm repository or `sync` and `override` access to an Application. Once a user has that access, different exploitation levels are possible depending on their other RBAC privileges. A patch for this vulnerability has been released in Argo CD versions 2.3.2, 2.2.8, and 2.1.14. Some mitigation measures are available but do not serve as a substitute for upgrading. To avoid privilege escalation, limit who has push access to Application source repositories or `sync` + `override` access to Applications; and limit which repositories are available in projects where users have `update` access to Applications. To avoid unauthorized resource inspection/tampering, limit who has `delete`, `get`, or `action` access to Applications.	9.9	More Details
CVE-2022-0479	The Popup Builder WordPress plugin before 4.1.1 does not sanitise and escape the sgpb-subscription-popup-id parameter before using it in a SQL statement in the All Subscribers admin dashboard, leading to a SQL injection, which could also be used to perform Reflected Cross-Site Scripting attack against a logged in admin opening a malicious link	9.8	More Details
CVE-2022-23884	Mojang Bedrock Dedicated Server 1.18.2 is affected by an integer overflow leading to a bound check bypass caused by PurchaseReceiptPacket::_read (packet deserializer).	9.8	More Details
CVE-2021-25070	The Block Bad Bots WordPress plugin before 6.88 does not properly sanitise and escape the User Agent before using it in a SQL statement to record logs, leading to an SQL Injection issue	9.8	More Details
CVE-2021-45756	Asus RT-AC68U <3.0.0.4.385.20633 and RT-AC5300 <3.0.0.4.384.82072 are affected by a buffer overflow in blocking_request.cgi.	9.8	More Details
CVE-2022-0679	The Narnoo Distributor WordPress plugin through 2.5.1 fails to validate and sanitize the lib_path parameter before it is passed into a call to require() via the narnoo_distributor_lib_request AJAX action (available to both unauthenticated and authenticated users) which results in the disclosure of arbitrary files as the content of the file is then displayed in the response as JSON data. This could also lead to RCE with various tricks but depends on the underlying system and it's configuration.	9.8	More Details
CVE-2022-0784	The Title Experiments Free WordPress plugin before 9.0.1 does not sanitise and escape the id parameter before using it in a SQL statement via the wpex_titles AJAX action (available to unauthenticated users), leading to an unauthenticated SQL injection	9.8	More Details
CVE-2022-0787	The Limit Login Attempts (Spam Protection) WordPress plugin before 5.1 does not sanitise and escape some parameters before using them in SQL statements via AJAX actions (available to unauthenticated users), leading to SQL Injections	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0846	The SpeakOut! Email Petitions WordPress plugin before 2.14.15.1 does not sanitise and escape the id parameter before using it in a SQL statement via the dk_speakout_sendmail AJAX action, leading to an SQL Injection exploitable by unauthenticated users	9.8	More Details
CVE-2022-0342	An authentication bypass vulnerability in the CGI program of Zyxel USG/ZyWALL series firmware versions 4.20 through 4.70, USG FLEX series firmware versions 4.50 through 5.20, ATP series firmware versions 4.32 through 5.20, VPN series firmware versions 4.30 through 5.20, and NSG series firmware versions V1.20 through V1.33 Patch 4, which could allow an attacker to bypass the web authentication and obtain administrative access of the device.	9.8	More Details
CVE-2022-26268	Xiaohuanxiong v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /app/controller/Books.php.	9.8	More Details
CVE-2022-23882	TuziCMS 2.0.6 is affected by SQL injection in \App\Manage\Controller\BannerController.class.php.	9.8	More Details
CVE-2022-25757	In Apache APISIX before 2.13.0, when decoding JSON with duplicate keys, lua-cjson will choose the last occurred value as the result. By passing a JSON with a duplicate key, the attacker can bypass the body_schema validation in the request-validation plugin. For example, `{"string_payload":"bad","string_payload":"good"}` can be used to hide the "bad" input. Systems satisfy three conditions below are affected by this attack: 1. use body_schema validation in the request-validation plugin 2. upstream application uses a special JSON library that chooses the first occurred value, like jsoniter or gojay 3. upstream application does not validate the input anymore. The fix in APISIX is to re-encode the validated JSON input back into the request body at the side of APISIX. Improper Input Validation vulnerability in __COMPONENT__ of Apache APISIX allows an attacker to __IMPACT__. This issue affects Apache APISIX Apache APISIX version 2.12.1 and prior versions.	9.8	More Details
CVE-2022-26273	EyouCMS v1.5.4 was discovered to lack parameter filtering in \user\controller\shop.php, leading to payment logic vulnerabilities.	9.8	More Details
CVE-2021-44617	A SQL Injection vulnerability exits in the Ramo plugin for GLPI 9.4.6 via the idu parameter in plugins/ramo/ramoapirest.php/getOutdated.	9.8	More Details
CVE-2021-45865	A File Upload vulnerability exists in Sourcecodester Student Attendance Manageent System 1.0 via the file upload functionality.	9.8	More Details
CVE-2021-26600	ImpressCMS before 1.4.3 has plugins/preloads/autologin.php type confusion with resultant Authentication Bypass (!= instead of !==).	9.8	More Details
CVE-2021-26599	ImpressCMS before 1.4.3 allows include/findusers.php groups SQL Injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26258	D-Link DIR-820L 1.05B03 was discovered to contain remote command execution (RCE) vulnerability via HTTP POST to get set ccp.	9.8	More Details
CVE-2022-26255	Clash for Windows v0.19.8 was discovered to allow arbitrary code execution via a crafted payload injected into the Proxies name column.	9.8	More Details
CVE-2022-26278	Tenda AC9 v15.03.2.21_cn was discovered to contain a stack overflow via the time parameter in the PowerSaveSet function.	9.8	More Details
CVE-2022-25347	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) is vulnerable to path traversal attacks, which may allow an attacker to write arbitrary files to locations on the file system.	9.8	More Details
CVE-2022-25521	NUUO v03.11.00 was discovered to contain access control issue.	9.8	More Details
CVE-2022-26349	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability that exists in DIAE_eccoefficientHandler.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2021-43118	A Remote Command Injection vulnerability exists in DrayTek Vigor 2960 1.5.1.3, DrayTek Vigor 3900 1.5.1.3, and DrayTek Vigor 300B 1.5.1.3 via a crafted HTTP message containing malformed QUERY STRING in mainfunction.cgi, which could let a remote malicious user execute arbitrary code.	9.8	More Details
CVE-2021-42911	A Format String vulnerability exists in DrayTek Vigor 2960 <= 1.5.1.3, DrayTek Vigor 3900 <= 1.5.1.3, and DrayTek Vigor 300B <= 1.5.1.3 in the mainfunction.cgi file via a crafted HTTP message containing malformed QUERY STRING, which could let a remote malicious user execute arbitrary code.	9.8	More Details
CVE-2021-43110	An Access Conrol vulnerability exists in PuneethReddyHC online-shopping-system as of 11/01/2021 in add_products.	9.8	More Details
CVE-2022-27175	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability that exists in GetCalcTagList. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-26887	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in DIAE_loopmapHandler.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-26836	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability that exists in HandlerExport.ashx/Calendar. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26667	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability that exists in GetDemandAnalysisData. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-26666	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in HandlerECC.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-26514	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability that exists in DIAE_tagHandler.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-26338	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in HandlerPageP_KID.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-25420	NTT Resonant Incorporated goo blog App Web Application 1.0 is vulnerable to CLRF injection. This vulnerability allows attackers to execute arbitrary code via a crafted HTTP request.	9.8	More Details
CVE-2022-26069	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability that exists in HandlerPage_KID.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-26065	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in GetLatestDemandNode. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-26059	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability that exists in GetQueryData. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-26013	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability that exists in DIAE_dmdsetHandler.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-25980	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability that exists in HandlerCommon.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-25880	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in HandlerTag_KID.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26245	Falcon-plus v0.3 was discovered to contain a SQL injection vulnerability via the parameter grpName in /config/service/host.go.	9.8	More Details
CVE-2022-0923	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability that exists in HandlerDialog_KID.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-23901	A stack overflow re2c 2.2 exists due to infinite recursion issues in src/dfa/dead_rules.cc.	9.8	More Details
CVE-2021-44127	In DLink DAP-1360 F1 firmware version <=v6.10 in the "webupg" binary, an attacker can use the "file" parameter to execute arbitrary system commands when the parameter is "name=deleteFile" after being authorized.	9.8	More Details
CVE-2022-22274	A Stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution in the firewall.	9.8	More Details
CVE-2022-27081	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/SetLanInfo.	9.8	More Details
CVE-2022-24934	wpsupdater.exe in Kingsoft WPS Office through 11.2.0.10382 allows remote code execution by modifying HKEY_CURRENT_USER in the registry.	9.8	More Details
CVE-2022-27080	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setWorkmode.	9.8	More Details
CVE-2022-27079	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setPicListItem.	9.8	More Details
CVE-2022-27078	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setAdInfoDetail.	9.8	More Details
CVE-2022-27077	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /cgi-bin/uploadWeiXinPic.	9.8	More Details
CVE-2022-27076	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/delAd.	9.8	More Details
CVE-2022-26536	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/setFixTools.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26290	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/WriteFacMac.	9.8	More Details
CVE-2022-26289	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/exeCommand.	9.8	More Details
CVE-2021-31326	D-Link DIR-816 A2 1.10 B05 allows unauthenticated attackers to arbitrarily reset the device via a crafted tokenid parameter to /goform/form2Reboot.cgi.	9.8	More Details
CVE-2022-23881	ZZZCMS zzzphp v2.1.0 was discovered to contain a remote command execution (RCE) vulnerability via danger_key() at zzz_template.php.	9.8	More Details
CVE-2022-27082	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /goform/SetInternetLanInfo.	9.8	More Details
CVE-2022-23880	An arbitrary file upload vulnerability in the File Management function module of taoCMS v3.0.2 allows attackers to execute arbitrary code via a crafted PHP file.	9.8	More Details
CVE-2022-25222	Money Transfer Management System Version 1.0 allows an unauthenticated user to inject SQL queries in 'admin/maintenance/manage_branch.php' and 'admin/maintenance/manage_fee.php' via the 'id' parameter.	9.8	More Details
CVE-2022-24293	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	9.8	More Details
CVE-2022-24292	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	9.8	More Details
CVE-2022-0888	The Ninja Forms - File Uploads Extension WordPress plugin is vulnerable to arbitrary file uploads due to insufficient input file type validation found in the ~/includes/ajax/controllers/uploads.php file which can be bypassed making it possible for unauthenticated attackers to upload malicious files that can be used to obtain remote code execution, in versions up to and including 3.3.0	9.8	More Details
CVE-2021-27428	GE UR IED firmware versions prior to version 8.1x supports upgrading firmware using UR Setup configuration tool – Enervista UR Setup. This UR Setup tool validates the authenticity and integrity of firmware file before uploading the UR IED. An illegitimate user could upgrade firmware without appropriate privileges. The weakness is assessed, and mitigation is implemented in firmware Version 8.10.	9.8	More Details
CVE-2021-27426	GE UR IED firmware versions prior to version 8.1x with “Basic” security variant does not allow the disabling of the “Factory Mode,” which is used for servicing the IED by a “Factory” user.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38278	Tenda AC10-1200 v15.03.06.23_EN was discovered to contain a buffer overflow via the urls parameter in the saveParentControlInfo function.	9.8	More Details
CVE-2021-43736	CmsWing CMS 1.3.7 is affected by a Remote Code Execution (RCE) vulnerability via parameter: log rule	9.8	More Details
CVE-2022-26205	Marky commit 3686565726c65756e was discovered to contain a remote code execution (RCE) vulnerability via the Display text fields. This vulnerability allows attackers to execute arbitrary code via injection of a crafted payload.	9.8	More Details
CVE-2022-26871	An arbitrary file upload vulnerability in Trend Micro Apex Central could allow an unauthenticated remote attacker to upload an arbitrary file which could lead to remote code execution.	9.8	More Details
CVE-2022-27083	Tenda M3 1.10 V1.0.0.12(4856) was discovered to contain a command injection vulnerability via the component /cgi-bin/uploadAccessCodePic.	9.8	More Details
CVE-2022-26301	TuziCMS v2.0.6 was discovered to contain a SQL injection vulnerability via the component App\Manage\Controller\ZhuantiController.class.php.	9.8	More Details
CVE-2022-26198	Notable v1.8.4 does not filter text editing, allowing attackers to execute arbitrary code via a crafted payload injected into the Title text field.	9.8	More Details
CVE-2021-43735	CmsWing 1.3.7 is affected by a SQLi vulnerability via parameter: behavior rule.	9.8	More Details
CVE-2022-27919	Gradle Enterprise before 2022.1 allows remote code execution if the installation process did not specify an initial configuration file. The configuration allows certain anonymous access to administration and an API.	9.8	More Details
CVE-2021-43636	Two Buffer Overflow vulnerabilities exists in T10 V2_Firmware V4.1.8cu.5207_B20210320 in the http_request_parse function when processing host data in the HTTP request process.	9.8	More Details
CVE-2021-43090	An XML External Entity (XXE) vulnerability exists in soa-model before 1.6.4 in the WSDLParser function.	9.8	More Details
CVE-2022-27811	GNOME OCRFeeder before 0.8.4 allows OS command injection via shell metacharacters in a PDF or image filename.	9.8	More Details
CVE-2022-22687	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in Authentication functionality in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to execute arbitrary code via unspecified vectors.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1040	An authentication bypass vulnerability in the User Portal and Webadmin allows a remote attacker to execute code in Sophos Firewall version v18.5 MR3 and older.	9.8	More Details
CVE-2022-26279	EyouCMS v1.5.5 was discovered to have no access control in the component /data/sqldata.	9.8	More Details
CVE-2022-26272	A remote code execution (RCE) vulnerability in Ionize v1.0.8.1 allows attackers to execute arbitrary code via a crafted string written to the file application/config/config.php.	9.8	More Details
CVE-2022-26249	Survey King v0.3.0 does not filter data properly when exporting excel files, allowing attackers to execute arbitrary code or access sensitive information via a CSV injection attack.	9.8	More Details
CVE-2021-43084	An SQL Injection vulnerability exists in Dreamer CMS 4.0.0 via the tableName parameter.	9.8	More Details
CVE-2021-43700	An issue was discovered in ApiManager 1.1. there is sql injection vulnerability that can use in /index.php?act=api&tag=8.	9.8	More Details
CVE-2021-26622	An remote code execution vulnerability due to SSTI vulnerability and insufficient file name parameter validation was discovered in Genian NAC. Remote attackers are able to execute arbitrary malicious code with SYSTEM privileges on all connected nodes in NAC through this vulnerability.	9.6	More Details
CVE-2022-22374	The BMC (IBM Power 9 AC922 OP910, OP920, OP930, and OP940) may be subject to a firmware downgrade attack which may affect its ability to operate its host. IBM X-Force ID: 221442.	9.1	More Details
CVE-2022-24303	Pillow before 9.0.1 allows attackers to delete files because spaces in temporary pathnames are mishandled.	9.1	More Details
CVE-2021-45490	The client applications in 3CX on Windows, the 3CX app for iOS, and the 3CX application for Android through 2022-03-17 lack SSL certificate validation.	9.1	More Details
CVE-2022-25577	ALF-BanCO v8.2.5 and below was discovered to use a hardcoded password to encrypt the SQLite database containing the user's data. Attackers who are able to gain remote or local access to the system are able to read and modify the data.	9.1	More Details
CVE-2022-22952	VMware Carbon Black App Control (8.5.x prior to 8.5.14, 8.6.x prior to 8.6.6, 8.7.x prior to 8.7.4 and 8.8.x prior to 8.8.2) contains a file upload vulnerability. A malicious actor with administrative access to the VMware App Control administration interface may be able to execute code on the Windows instance where AppC Server is installed by uploading a specially crafted file.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22951	VMware Carbon Black App Control (8.5.x prior to 8.5.14, 8.6.x prior to 8.6.6, 8.7.x prior to 8.7.4 and 8.8.x prior to 8.8.2) contains an OS command injection vulnerability. An authenticated, high privileged malicious actor with network access to the VMware App Control administration interface may be able to execute commands on the server due to improper input validation leading to remote code execution.	9.1	More Details
CVE-2022-26629	An Access Control vulnerability exists in SoroushPlus+ Messenger 1.0.30 in the Lock Screen Security Feature function due to insufficient permissions and privileges, which allows a malicious attacker bypass the lock screen function.	9.1	More Details
CVE-2021-46743	In Firebase PHP-JWT before 6.0.0, an algorithm-confusion issue (e.g., RS256 / HS256) exists via the kid (aka Key ID) header, when multiple types of keys are loaded in a key ring. This allows an attacker to forge tokens that validate under the incorrect key. NOTE: this provides a straightforward way to use the PHP-JWT library unsafely, but might not be considered a vulnerability in the library itself.	9.1	More Details
CVE-2022-1106	use after free in mrb_vm_exec in GitHub repository mruby/mruby prior to 3.2.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-43738	An issue was discovered in xiaohuanxiong CMS 5.0.17. There is a CSRF vulnerability that can that can add the administrator account.	8.8	More Details
CVE-2022-28136	A cross-site request forgery (CSRF) vulnerability in Jenkins JiraTestResultReporter Plugin 165.v817928553942 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials.	8.8	More Details
CVE-2021-40905	The web management console of CheckMK Enterprise Edition (versions 1.5.0 to 2.0.0p9) does not properly sanitise the uploading of ".mkp" files, which are Extension Packages, making remote code execution possible. Successful exploitation requires access to the web management interface, either with valid credentials or with a hijacked session of a user with administrator role. NOTE: the vendor states that this is the intended behavior: admins are supposed to be able to execute code in this manner	8.8	More Details
CVE-2022-25523	TypesetterCMS v5.1 was discovered to contain a Cross-Site Request Forgery (CSRF) which is exploited via a crafted POST request.	8.8	More Details
CVE-2022-1049	A flaw was found in the Pacemaker configuration tool (pcs). The pcs daemon was allowing expired accounts, and accounts with expired passwords to login when using PAM authentication. Therefore, unprivileged expired accounts that have been denied access could still login.	8.8	More Details
CVE-2022-27945	NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the sysNewPasswd and sysConfirmPasswd parameters to password.cgi.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27946	NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the sysNewPasswd and sysConfirmPasswd parameters to admin_account.cgi.	8.8	More Details
CVE-2022-27947	NETGEAR R8500 1.0.2.158 devices allow remote authenticated users to execute arbitrary commands (such as telnetd) via shell metacharacters in the ipv6_fix.cgi ipv6_wan_ipaddr, ipv6_lan_ipaddr, ipv6_wan_length, or ipv6_lan_length parameter.	8.8	More Details
CVE-2022-0983	An SQL injection risk was identified in Badges code relating to configuring criteria. Access to the relevant capability was limited to teachers and managers by default.	8.8	More Details
CVE-2022-0435	A stack overflow flaw was found in the Linux kernel's TIPC protocol functionality in the way a user sends a packet with malicious content where the number of domain member nodes is higher than the 64 allowed. This flaw allows a remote user to crash the system or possibly escalate their privileges if they have access to the TIPC network.	8.8	More Details
CVE-2021-24962	The WordPress File Upload Free and Pro WordPress plugins before 4.16.3 allow users with a role as low as Contributor to perform path traversal via a shortcode argument, which can then be used to upload a PHP code disguised as an image inside the auto-loaded directory of the plugin, resulting in arbitrary code execution.	8.8	More Details
CVE-2022-0499	The Sermon Browser WordPress plugin through 0.45.22 does not have CSRF checks in place when uploading Sermon files, and does not validate them in any way, allowing attackers to make a logged in admin upload arbitrary files such as PHP ones.	8.8	More Details
CVE-2022-0770	The Translate WordPress with GTranslate WordPress plugin before 2.9.9 does not have CSRF check in some files, and write debug data such as user's cookies in a publicly accessible file if a specific parameter is used when requesting them. Combining those two issues, an attacker could gain access to a logged in admin cookies by making them open a malicious link or page	8.8	More Details
CVE-2021-40904	The web management console of CheckMK Raw Edition (versions 1.5.0 to 1.6.0) allows a misconfiguration of the web-app Dokuwiki (installed by default), which allows embedded php code. As a result, remote code execution is achieved. Successful exploitation requires access to the web management interface, either with valid credentials or with a hijacked session by a user with the role of administrator.	8.8	More Details
CVE-2022-22934	An issue was discovered in SaltStack Salt in versions before 3002.8, 3003.4, 3004.1. Salt Masters do not sign pillar data with the minion’s public key, which can result in attackers substituting arbitrary pillar data.	8.8	More Details
CVE-2022-28150	A cross-site request forgery (CSRF) vulnerability in Jenkins Job and Node ownership Plugin 0.13.0 and earlier allows attackers to change the owners and item-specific permissions of a job.	8.8	More Details
CVE-2022-0981	A flaw was found in Quarkus. The state and potentially associated permissions can leak from one web request to another in RestEasy Reactive. This flaw allows a low-privileged user to perform operations on the database with a different set of privileges than intended.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1030	Okta Advanced Server Access Client for Linux and macOS prior to version 1.58.0 was found to be vulnerable to command injection via a specially crafted URL. An attacker, who has knowledge of a valid team name for the victim and also knows a valid target host where the user has access, can execute commands on the local system.	8.8	More Details
CVE-2022-1064	SQL injection through marking blog comments on bulk as spam in GitHub repository forkcms/forkcms prior to 5.11.1.	8.8	More Details
CVE-2022-1050	A flaw was found in the QEMU implementation of VMWare's paravirtual RDMA device. This flaw allows a crafted guest driver to execute HW commands when shared buffers are not yet allocated, potentially leading to a use-after-free condition.	8.8	More Details
CVE-2022-22688	Improper neutralization of special elements used in a command ('Command Injection') vulnerability in File service functionality in Synology DiskStation Manager (DSM) before 6.2.4-25556-2 allows remote authenticated users to execute arbitrary commands via unspecified vectors.	8.8	More Details
CVE-2022-22936	An issue was discovered in SaltStack Salt in versions before 3002.8, 3003.4, 3004.1. Job publishes and file server replies are susceptible to replay attacks, which can result in an attacker replaying job publishes causing minions to run old jobs. File server replies can also be re-played. A sufficient craft attacker could gain root access on minion under certain scenarios.	8.8	More Details
CVE-2022-22941	An issue was discovered in SaltStack Salt in versions before 3002.8, 3003.4, 3004.1. When configured as a Master-of-Masters, with a publisher_acl, if a user configured in the publisher_acl targets any minion connected to the Syndic, the Salt Master incorrectly interpreted no valid targets as valid, allowing configured users to target any of the minions connected to the syndic with their configured commands. This requires a syndic master combined with publisher_acl configured on the Master-of-Masters, allowing users specified in the publisher_acl to bypass permissions, publishing authorized commands to any configured minion.	8.8	More Details
CVE-2022-25267	Password On-Premise Edition before 4.6.13 allows migration/uploadExportFile Directory Traversal (to upload files).	8.8	More Details
CVE-2022-25268	Password On-Premise Edition before 4.6.13 allows CSRF via the groups, password, and history subsystems.	8.8	More Details
CVE-2021-27475	Rockwell Automation Connected Components Workbench v12.00.00 and prior does not limit the objects that can be deserialized. This vulnerability allows attackers to craft a malicious serialized object that, if opened by a local user in Connected Components Workbench, may result in remote code execution. This vulnerability requires user interaction to be successfully exploited.	8.6	More Details
CVE-2021-27430	GE UR bootloader binary Version 7.00, 7.01 and 7.02 included unused hardcoded credentials. Additionally, a user with physical access to the UR IED can interrupt the boot sequence by rebooting the UR.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44082	textpattern 4.8.7 is vulnerable to Cross Site Scripting (XSS) via /textpattern/index.php,Body. A remote and unauthenticated attacker can use XSS to trigger remote code execution by uploading a webshell. To do so they must first steal the CSRF token before submitting a file upload request.	8.3	More Details
CVE-2021-44683	The DuckDuckGo browser 7.64.4 on iOS allows Address Bar Spoofing due to mishandling of the JavaScript window.open function (used to open a secondary browser window). This could be exploited by tricking users into supplying sensitive information such as credentials, because the address bar would display a legitimate URL, but content would be hosted on the attacker's web site.	8.2	More Details
CVE-2021-44905	Incorrect permissions in the Bluetooth Services in the Fortessa FTBTLD Smart Lock as of 12-13-2022 allows a remote attacker to disable the lock via an unauthenticated edit to the lock name.	8.2	More Details
CVE-2021-35254	SolarWinds received a report of a vulnerability related to an input that was not sanitized in WebHelpDesk. SolarWinds has removed this input field to prevent the misuse of this input in the future.	8.2	More Details
CVE-2022-1071	User after free in mrb_vm_exec in GitHub repository mruby/mruby prior to 3.2.	8.2	More Details
CVE-2022-28154	Jenkins Coverage/Complexity Scatter Plot Plugin 1.1.1 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	8.1	More Details
CVE-2021-44759	Improper Authentication vulnerability in TLS origin validation of Apache Traffic Server allows an attacker to create a man in the middle attack. This issue affects Apache Traffic Server 8.0.0 to 8.1.0.	8.1	More Details
CVE-2021-26601	ImpressCMS before 1.4.3 allows libraries/image-editor/image-edit.php image_temp Directory Traversal.	8.1	More Details
CVE-2022-0759	A flaw was found in all versions of kubeclient up to (but not including) v4.9.3, the Ruby client for Kubernetes REST API, in the way it parsed kubeconfig files. When the kubeconfig file does not configure custom CA to verify certs, kubeclient ends up accepting any certificate (it wrongly returns VERIFY_NONE). Ruby applications that leverage kubeclient to parse kubeconfig files are susceptible to Man-in-the-middle attacks (MITM).	8.1	More Details
CVE-2020-21554	A File Deletion vulnerability exists in TinyShop 3.1.1 in the back_list parameter in controllers\admin.php, which could let a malicious user delete any file such as install.lock to reinstall cms.	8.1	More Details
CVE-2022-28155	Jenkins Pipeline: Phoenix AutoTest Plugin 1.3 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26621	An Buffer Overflow vulnerability leading to remote code execution was discovered in MEX01. Remote attackers can use this vulnerability by using the property that the target program copies parameter values to memory through the strcpy() function.	8.1	More Details
CVE-2022-28140	Jenkins Flaky Test Handler Plugin 1.2.1 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	8.1	More Details
CVE-2021-3589	An authorization flaw was found in Foreman Ansible. An authenticated attacker with certain permissions to create and run Ansible jobs can access hosts through job templates. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	8.0	More Details
CVE-2021-4157	An out of memory bounds write flaw (1 or 2 bytes of memory) in the Linux kernel NFS subsystem was found in the way users use mirroring (replication of files with NFS). A user, having access to the NFS mount, could potentially use this flaw to crash the system or escalate privileges on the system.	8.0	More Details
CVE-2022-22819	NXP LPC55S66JBD64, LPC55S66JBD100, LPC55S66JEV98, LPC55S69JBD64, LPC55S69JBD100, and LPC55S69JEV98 microcontrollers (ROM version 1B) have a buffer overflow in parsing SB2 updates before the signature is verified. This can allow an attacker to achieve non-persistent code execution via a crafted unsigned update.	7.8	More Details
CVE-2022-21821	NVIDIA CUDA Toolkit SDK contains an integer overflow vulnerability in cuobjdump.To exploit this vulnerability, a remote attacker would require a local user to download a specially crafted, corrupted file and locally execute cuobjdump against the file. Such an attack may lead to remote code execution that causes complete denial of service and an impact on data confidentiality and integrity.	7.8	More Details
CVE-2022-26839	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) is vulnerable to an incorrect default permission in the DIAEnergie application, which may allow an attacker to plant new files (such as DLLs) or replace existing executable files.	7.8	More Details
CVE-2022-1055	A use-after-free exists in the Linux Kernel in tc_new_tfilter that could allow a local attacker to gain privilege escalation. The exploit requires unprivileged user namespaces. We recommend upgrading past commit 04c2a47ffb13c29778e2a14e414ad4cb5a5db4b5	7.8	More Details
CVE-2021-44462	This vulnerability can be exploited by parsing maliciously crafted project files with Horner Automation Cscape EnvisionRV v4.50.3.1 and prior. The issues result from the lack of proper validation of user-supplied data, which can result in reads and writes past the end of allocated data structures. User interaction is required to exploit this vulnerability as an attacker must trick a valid user to open a malicious HMI project file.	7.8	More Details
CVE-2021-28277	A Heap-based Buffer Overflow vulnerabilty exists in jhead 3.04 and 3.05 is affected by: Buffer Overflow via the RemoveUnknownSections function in jpgfile.c.	7.8	More Details
CVE-2022-0330	A random memory access flaw was found in the Linux kernel's GPU i915 kernel driver functionality in the way a user may run malicious code on the GPU. This flaw allows a local user to crash the system or escalate their privileges on the system.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26259	A buffer over flow in Xiongmai DVR devices NBD80X16S-KL, NBD80X09S-KL, NBD80X08S-KL, NBD80X09RA-KL, AHB80X04R-MH, AHB80X04R-MH-V2, AHB80X04-R-MH-V3, AHB80N16T-GS, AHB80N32F4-LME, and NBD90S0VT-QW allows attackers to cause a Denial of Service (DoS) via a crafted RSTP request.	7.8	More Details
CVE-2022-0500	A flaw was found in unrestricted eBPF usage by the BPF_BTF_LOAD, leading to a possible out-of-bounds memory write in the Linux kernel's BPF subsystem due to the way a user loads BTF. This flaw allows a local user to crash or escalate their privileges on the system.	7.8	More Details
CVE-2022-0995	An out-of-bounds (OOB) memory write flaw was found in the Linux kernel's watch_queue event notification subsystem. This flaw can overwrite parts of the kernel state, potentially allowing a local user to gain privileged access or cause a denial of service on the system.	7.8	More Details
CVE-2022-1033	Unrestricted Upload of File with Dangerous Type in GitHub repository crater-invoice/crater prior to 6.0.6.	7.8	More Details
CVE-2022-27941	tcprewrite in Tcpreplay 4.4.1 has a heap-based buffer over-read in get_l2len_protocol in common/get.c.	7.8	More Details
CVE-2022-27940	tcprewrite in Tcpreplay 4.4.1 has a heap-based buffer over-read in get_ipv6_next in common/get.c.	7.8	More Details
CVE-2021-28278	A Heap-based Buffer Overflow vulnerability exists in jhead 3.04 and 3.05 via the RemoveSectionType function in jpgfile.c.	7.8	More Details
CVE-2022-27666	A heap buffer overflow flaw was found in IPsec ESP transformation code in net/ipv4/esp4.c and net/ipv6/esp6.c. This flaw allows a local attacker with a normal user privilege to overwrite kernel heap objects and may cause a local privilege escalation threat.	7.8	More Details
CVE-2022-27942	tcpprep in Tcpreplay 4.4.1 has a heap-based buffer over-read in parse_mpls in common/get.c.	7.8	More Details
CVE-2021-4197	An unprivileged write to the file handler flaw in the Linux kernel's control groups and namespaces subsystem was found in the way users have access to some less privileged process that are controlled by cgroups and have higher privileged parent process. It is actually both for cgroup2 and cgroup1 versions of control groups. A local user could use this flaw to crash the system or escalate their privileges on the system.	7.8	More Details
CVE-2021-46064	IrfanView 4.59 is vulnerable to buffer overflow via the function at address 0x413c70 (in 32bit version of the binary). The vulnerability triggers when the user opens malicious .tiff image.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0427	Missing sanitization of HTML attributes in Jupyter notebooks in all versions of GitLab CE/EE since version 14.5 allows an attacker to perform arbitrary HTTP POST requests on a user's behalf leading to potential account takeover	7.7	More Details
CVE-2022-24730	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Argo CD starting with version 1.3.0 but before versions 2.1.11, 2.2.6, and 2.3.0 is vulnerable to a path traversal bug, compounded by an improper access control bug, allowing a malicious user with read-only repository access to leak sensitive files from Argo CD's repo-server. A malicious Argo CD user who has been granted `get` access for a repository containing a Helm chart can craft an API request to the `/api/v1/repositories/{repo_url}/appdetails` endpoint to leak the contents of out-of-bounds files from the repo-server. The malicious payload would reference an out-of-bounds file, and the contents of that file would be returned as part of the response. Contents from a non-YAML file may be returned as part of an error message. The attacker would have to know or guess the location of the target file. Sensitive files which could be leaked include files from other Applications' source repositories or any secrets which have been mounted as files on the repo-server. This vulnerability is patched in Argo CD versions 2.1.11, 2.2.6, and 2.3.0. The patches prevent path traversal and limit access to users who either A) have been granted Application `create` privileges or B) have been granted Application `get` privileges and are requesting details for a `repo_url` that has already been used for the given Application. There are currently no known workarounds.	7.7	More Details
CVE-2021-27471	The parsing mechanism that processes certain file types does not provide input sanitization for file paths. This may allow an attacker to craft malicious files that, when opened by Rockwell Automation Connected Components Workbench v12.00.00 and prior, can traverse the file system. If successfully exploited, an attacker could overwrite existing files and create additional files with the same permissions of the Connected Components Workbench software. User interaction is required for this exploit to be successful.	7.7	More Details
CVE-2022-24789	C1 CMS is an open-source, .NET based Content Management System (CMS). Versions prior to 6.12 allow an authenticated user to exploit Server Side Request Forgery (SSRF) by causing the server to make arbitrary GET requests to other servers in the local network or on localhost. The attacker may also truncate arbitrary files to zero size (effectively delete them) leading to denial of service (DoS) or altering application logic. The authenticated user may unknowingly perform the actions by visiting a specially crafted site. Patched in C1 CMS v6.12, no known workarounds exist.	7.6	More Details
CVE-2021-44477	GE Gas Power ToolBoxST Version v04.07.05C suffers from an XML external entity (XXE) vulnerability using the DTD parameter entities technique that could result in disclosure and retrieval of arbitrary data on the affected node via an out-of-band (OOB) attack. The vulnerability is triggered when input passed to the XML parser is not sanitized while parsing the XML project/template file.	7.5	More Details
CVE-2021-3814	It was found that 3scale's APIdocs does not validate the access token, in the case of invalid token, it uses session auth instead. This conceivably bypasses access controls and permits unauthorized information disclosure.	7.5	More Details
CVE-2021-3567	A flaw was found in Caribou due to a regression of CVE-2020-25712 fix. An attacker could use this flaw to bypass screen-locking applications that leverage Caribou as an input mechanism. The highest threat from this vulnerability is to system availability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3422	The lack of validation of a key-value field in the Splunk-to-Splunk protocol results in a denial-of-service in Splunk Enterprise instances configured to index Universal Forwarder traffic. The vulnerability impacts Splunk Enterprise versions before 7.3.9, 8.0 versions before 8.0.9, and 8.1 versions before 8.1.3. It does not impact Universal Forwarders. When Splunk forwarding is secured using TLS or a Token, the attack requires compromising the certificate or token, or both. Implementation of either or both reduces the severity to Medium.	7.5	More Details
CVE-2021-26620	An improper authentication vulnerability leading to information leakage was discovered in iptime NAS2dual. Remote attackers are able to steal important information in the server by exploiting vulnerabilities such as insufficient authentication when accessing the shared folder and changing user's passwords.	7.5	More Details
CVE-2022-27882	slaacd in OpenBSD 6.9 and 7.0 before 2022-03-22 has an integer signedness error and resultant heap-based buffer overflow triggerable by a crafted IPv6 router advertisement. NOTE: privilege separation and pledge can prevent exploitation.	7.5	More Details
CVE-2022-27881	engine.c in slaacd in OpenBSD 6.9 and 7.0 before 2022-02-21 has a buffer overflow triggerable by an IPv6 router advertisement with more than seven nameservers. NOTE: privilege separation and pledge can prevent exploitation.	7.5	More Details
CVE-2022-24778	The imgcrypt library provides API exensions for containerd to support encrypted container images and implements the ctd-decoder command line tool for use by containerd to decrypt encrypted container images. The imgcrypt function `CheckAuthorization` is supposed to check whether the current used is authorized to access an encrypted image and prevent the user from running an image that another user previously decrypted on the same system. In versions prior to 1.1.4, a failure occurs when an image with a ManifestList is used and the architecture of the local host is not the first one in the ManifestList. Only the first architecture in the list was tested, which may not have its layers available locally since it could not be run on the host architecture. Therefore, the verdict on unavailable layers was that the image could be run anticipating that image run failure would occur later due to the layers not being available. However, this verdict to allow the image to run enabled other architectures in the ManifestList to run an image without providing keys if that image had previously been decrypted. A patch has been applied to imgcrypt 1.1.4. Workarounds may include usage of different namespaces for each remote user.	7.5	More Details
CVE-2022-24777	grpc-swift is the Swift language implementation of gRPC, a remote procedure call (RPC) framework. Prior to version 1.7.2, a grpc-swift server is vulnerable to a denial of service attack via a reachable assertion. This is due to incorrect logic when handling GOAWAY frames. The attack is low-effort: it takes very little resources to construct and send the required sequence of frames. The impact on availability is high as the server will crash, dropping all in flight connections and requests. This issue is fixed in version 1.7.2. There are currently no known workarounds.	7.5	More Details
CVE-2021-43091	An SQL Injection vlnerability exits in Yeswiki doryphore 20211012 via the email parameter in the registration form.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24291	Certain HP Print devices may be vulnerable to potential information disclosure, denial of service, or remote code execution.	7.5	More Details
CVE-2022-27227	In PowerDNS Authoritative Server before 4.4.3, 4.5.x before 4.5.4, and 4.6.x before 4.6.1 and PowerDNS Recursor before 4.4.8, 4.5.x before 4.5.8, and 4.6.x before 4.6.1, insufficient validation of an IXFR end condition causes incomplete zone transfers to be handled as successful transfers.	7.5	More Details
CVE-2021-3748	A use-after-free vulnerability was found in the virtio-net device of QEMU. It could occur when the descriptor's address belongs to the non direct access region, due to num_buffers being set after the virtqueue elem has been unmapped. A malicious guest could use this flaw to crash QEMU, resulting in a denial of service condition, or potentially execute code on the host with the privileges of the QEMU process.	7.5	More Details
CVE-2022-26243	Tenda AC10-1200 v15.03.06.23_EN was discovered to contain a buffer overflow in the setSmartPowerManagement function.	7.5	More Details
CVE-2021-27422	GE UR firmware versions prior to version 8.1x web server interface is supported on UR over HTTP protocol. It allows sensitive information exposure without authentication.	7.5	More Details
CVE-2022-25571	Bluedon Information Security Technologies Co.,Ltd Internet Access Detector v1.0 was discovered to contain an information leak which allows attackers to access the contents of the password file via unspecified vectors.	7.5	More Details
CVE-2021-38772	Tenda AC10-1200 v15.03.06.23_EN was discovered to contain a buffer overflow via the list parameter in the fromSetIpMacBind function.	7.5	More Details
CVE-2022-26271	74cmsSE v3.4.1 was discovered to contain an arbitrary file read vulnerability via the $url parameter at \index\controller\Download.php.	7.5	More Details
CVE-2021-44124	Hiby Music Hiby OS R3 Pro 1.5 and 1.6 is vulnerable to Directory Traversal. The HTTP Server does not have enough input data sanitization when shown data from SD Card, an attacker can navigate through the device's File System over HTTP.	7.5	More Details
CVE-2021-44139	Sentinel 1.8.2 is vulnerable to Server-side request forgery (SSRF).	7.5	More Details
CVE-2022-27658	Under certain conditions, SAP Innovation management - version 2.0, allows an attacker to access information which could lead to information gathering for further exploits and attacks.	7.5	More Details
CVE-2021-44581	An SQL Injection vulnerabilty exists in Kreado Kreasfero 1.5 via the id parameter.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28142	Jenkins Proxmox Plugin 0.6.0 and earlier disables SSL/TLS certificate validation globally for the Jenkins controller JVM when configured to ignore SSL/TLS issues.	7.5	More Details
CVE-2021-44081	A buffer overflow vulnerability exists in the AMF of open5gs 2.1.4. When the length of MSIN in Supi exceeds 24 characters, it leads to AMF denial of service.	7.5	More Details
CVE-2021-44040	Improper Input Validation vulnerability in request line parsing of Apache Traffic Server allows an attacker to send invalid requests. This issue affects Apache Traffic Server 8.0.0 to 8.1.3 and 9.0.0 to 9.1.1.	7.5	More Details
CVE-2022-0635	Versions affected: BIND 9.18.0 When a vulnerable version of named receives a series of specific queries, the named process will eventually terminate due to a failed assertion check.	7.5	More Details
CVE-2021-43109	An SQL Injection vulnerability exits in PuneethReddyHC online-shopping-system as of 11/01/2021 via the p parameter in product.php.	7.5	More Details
CVE-2021-45757	ASUS AC68U <=3.0.0.4.385.20852 is affected by a buffer overflow in blocking.cgi, which may cause a denial of service (DoS).	7.5	More Details
CVE-2018-25032	zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches.	7.5	More Details
CVE-2021-28276	A Denial of Service vulnerability exists in jhead 3.04 and 3.05 via a wild address read in the ProcessCanonMakerNoteDir function in makernote.c.	7.5	More Details
CVE-2022-0315	Insecure Temporary File in GitHub repository horovod/horovod prior to 0.24.0.	7.5	More Details
CVE-2022-25568	MotionEye v0.42.1 and below allows attackers to access sensitive information via a GET request to /config/list. To exploit this vulnerability, a regular user password must be unconfigured.	7.5	More Details
CVE-2022-1061	Heap Buffer Overflow in parseDragons in GitHub repository radareorg/radare2 prior to 5.6.8.	7.5	More Details
CVE-2022-27192	The Reporting module in Aseco Lietuva document management system DVS Avilys before 3.5.58 allows unauthorized file download. An unauthenticated attacker can impersonate an administrator by reading administrative files.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24757	The Jupyter Server provides the backend (i.e. the core services, APIs, and REST endpoints) for Jupyter web applications. Prior to version 1.15.4, unauthorized actors can access sensitive information from server logs. Anytime a 5xx error is triggered, the auth cookie and other header values are recorded in Jupyter Server logs by default. Considering these logs do not require root access, an attacker can monitor these logs, steal sensitive auth/cookie information, and gain access to the Jupyter server. Jupyter Server version 1.15.4 contains a patch for this issue. There are currently no known workarounds.	7.5	More Details
CVE-2021-43666	A Denial of Service vulnerability exists in mbed TLS 3.0.0 and earlier in the mbedtls_pkcs12_derivation function when an input password's length is 0.	7.5	More Details
CVE-2022-0153	SQL Injection in GitHub repository forkcms/forkcms prior to 5.11.1.	7.5	More Details
CVE-2021-3618	ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.	7.4	More Details
CVE-2021-44226	Razer Synapse before 3.7.0228.022817 allows privilege escalation because it relies on %PROGRAMDATA%\Razer\Synapse3\Service\bin even if %PROGRAMDATA%\Razer has been created by any unprivileged user before Synapse is installed. The unprivileged user may have placed Trojan horse DLLs there.	7.3	More Details
CVE-2022-1073	A vulnerability was found in Automatic Question Paper Generator 1.0. It has been declared as critical. An attack leads to privilege escalation. The attack can be launched remotely.	7.3	More Details
CVE-2022-1080	A vulnerability was found in SourceCodester One Church Management System 1.0. It has been declared as critical. This vulnerability affects code of the file attendancy.php as the manipulation of the argument search2 leads to sql injection. The attack can be initiated remotely.	7.3	More Details
CVE-2022-1082	A vulnerability was found in SourceCodester Microfinance Management System 1.0. It has been rated as critical. This issue affects the file /mims/login.php of the Login Page. The manipulation of the argument username/password with the input 'll1=1# leads to sql injection. The attack may be initiated remotely.	7.3	More Details
CVE-2022-1083	A vulnerability classified as critical has been found in Microfinance Management System. The manipulation of arguments like customer_type_number/account_number/account_status_number/account_type_number with the input ' and (select * from(select(sleep(10)))Avx) and 'abc' = 'abc leads to sql injection in multiple files. It is possible to launch the attack remotely.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1084	A vulnerability classified as critical was found in SourceCodester One Church Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /one_church/userregister.php. The manipulation leads to authentication bypass. The attack can be launched remotely.	7.3	More Details
CVE-2022-1078	A vulnerability was found in SourceCodester College Website Management System 1.0. It has been classified as critical. Affected is the file /cwms/admin/?page=articles/view_article/. The manipulation of the argument id with the input ' and (select * from(select(sleep(10)))Avx) and 'abc' = 'abc with an unknown input leads to sql injection. It is possible to launch the attack remotely and without authentication.	7.3	More Details
CVE-2022-1032	Insecure deserialization of not validated module file in GitHub repository crater-invoice/crater prior to 6.0.6.	7.2	More Details
CVE-2022-0550	Improper Input Validation vulnerability in custom report logo upload in Nozomi Networks Guardian, and CMC allows an authenticated attacker with admin or report manager roles to execute unattended commands on the appliance using web server user privileges. This issue affects: Nozomi Networks Guardian versions prior to 22.0.0. Nozomi Networks CMC versions prior to 22.0.0.	7.2	More Details
CVE-2022-26642	TP-LINK TL-WR840N(ES)_V6.20 was discovered to contain a buffer overflow via the X_TP_ClonedMACAddress parameter.	7.2	More Details
CVE-2022-26641	TP-LINK TL-WR840N(ES)_V6.20 was discovered to contain a buffer overflow via the httpRemotePort parameter.	7.2	More Details
CVE-2022-26640	TP-LINK TL-WR840N(ES)_V6.20 was discovered to contain a buffer overflow via the minAddress parameter.	7.2	More Details
CVE-2022-26639	TP-LINK TL-WR840N(ES)_V6.20 was discovered to contain a buffer overflow via the DNSServers parameter.	7.2	More Details
CVE-2021-43103	A File Upload vulnerability exists in bbs 5.3 is via ForumManageAction.java in a GetType function, which lets a remote malicious user execute arbitrary code.	7.2	More Details
CVE-2021-43102	A File Upload vulnerability exists in bbs 5.3 is via HelpManageAction.java in a GetType function, which lets a remote malicious user execute arbitrary code.	7.2	More Details
CVE-2021-43101	A File Upload vulnerability exists in bbs 5.3 is via MembershipCardManageAction.java in a GetType function, which lets a remote malicious user execute arbitrary code.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0834	The Amelia WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the lastName parameter found in the ~/src/Application/Controller/User/Customer/AddCustomerController.php file which allows attackers to inject arbitrary web scripts onto a pages that executes whenever a user accesses the booking calendar with the date the attacker has injected the malicious payload into. This affects versions up to and including 1.0.46.	7.2	More Details
CVE-2021-43100	A File Upload vulnerability exists in bbs 5.3 is via TopicManageAction.java in a GetType function, which lets a remote malicious user execute arbitrary code.	7.2	More Details
CVE-2021-43097	A Server-side Template Injection (SSTI) vulnerability exists in bbs 5.3 in TemplateManageAction.javawhich could let a malicoius user execute arbitrary code.	7.2	More Details
CVE-2021-43098	A File Upload vulnerability exists in bbs v5.3 via QuestionManageAction.java in a getType function.	7.2	More Details
CVE-2021-25064	The Wow Countdowns WordPress plugin through 3.1.2 does not sanitize user input into the 'did' parameter and uses it in a SQL statement, leading to an authenticated SQL Injection.	7.2	More Details
CVE-2022-0889	The Ninja Forms - File Uploads Extension WordPress plugin is vulnerable to reflected cross-site scripting due to missing sanitization of the files filename parameter found in the ~/includes/ajax/controllers/uploads.php file which can be used by unauthenticated attackers to add malicious web scripts to vulnerable WordPress sites, in versions up to and including 3.3.12.	7.2	More Details
CVE-2022-27948	Certain Tesla vehicles through 2022-03-26 allow attackers to open the charging port via a 315 MHz RF signal containing a fixed sequence of approximately one hundred symbols. NOTE: the vendor's perspective is that the behavior is as intended	7.2	More Details
CVE-2022-0551	Improper Input Validation vulnerability in project file upload in Nozomi Networks Guardian and CMC allows an authenticated attacker with admin or import manager roles to execute unattended commands on the appliance using web server user privileges. This issue affects: Nozomi Networks Guardian versions prior to 22.0.0. Nozomi Networks CMC versions prior to 22.0.0.	7.2	More Details
CVE-2021-25068	The Sync WooCommerce Product feed to Google Shopping WordPress plugin through 1.2.4 uses the 'feed_id' POST parameter which is not properly sanitized for use in a SQL statement, leading to a SQL injection vulnerability in the admin dashboard	7.2	More Details
CVE-2022-0988	Delta Electronics DIAEnergie (Version 1.7.5 and prior) is vulnerable to cleartext transmission as the web application runs by default on HTTP. This could allow an attacker to remotely read transmitted information between the client and product.	7.1	More Details
CVE-2021-4156	An out-of-bounds read flaw was found in libsndfile's FLAC codec functionality. An attacker who is able to submit a specially crafted file (via tricking a user to open or otherwise) to an application linked with libsndfile and using the FLAC codec, could trigger an out-of-bounds read that would most likely cause a crash but could potentially leak memory information that could be used in further exploitation of other flaws.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26659	Docker Desktop installer on Windows in versions before 4.6.0 allows an attacker to overwrite any administrator writable files by creating a symlink in place of where the installer writes its log file. Starting from version 4.6.0, the Docker Desktop installer, when run elevated, will write its log files to a location not writable by non-administrator users.	7.1	More Details
CVE-2022-24781	Geon is a board game based on solving questions about the Pythagorean Theorem. Malicious users can obtain the uuid from other users, spoof that uuid through the browser console and become co-owners of the target session. This issue is patched in version 1.1.0. No known workaround exists.	7.1	More Details
CVE-2021-4202	A use-after-free flaw was found in nci_request in net/nfc/nci/core.c in NFC Controller Interface (NCI) in the Linux kernel. This flaw could allow a local attacker with user privileges to cause a data race problem while the device is getting removed, leading to a privilege escalation problem.	7.0	More Details
CVE-2021-4203	A use-after-free read flaw was found in sock_getsockopt() in net/core/sock.c due to SO_PEERCRED and SO_PEERGROUPS race with listen() (and connect()) in the Linux kernel. In this flaw, an attacker with a user privileges may crash the system or leak internal kernel information.	6.8	More Details
CVE-2022-24731	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Argo CD starting with version 1.5.0 but before versions 2.1.11, 2.2.6, and 2.3.0 is vulnerable to a path traversal vulnerability, allowing a malicious user with read/write access to leak sensitive files from Argo CD's repo-server. A malicious Argo CD user who has been granted `create` or `update` access to Applications can leak the contents of any text file on the repo-server. By crafting a malicious Helm chart and using it in an Application, the attacker can retrieve the sensitive file's contents either as part of the generated manifests or in an error message. The attacker would have to know or guess the location of the target file. Sensitive files which could be leaked include files from another Application's source repositories or any secrets which have been mounted as files on the repo-server. This vulnerability is patched in Argo CD versions 2.1.11, 2.2.6, and 2.3.0. The problem can be mitigated by avoiding storing secrets in git, avoiding mounting secrets as files on the repo-server, avoiding decrypting secrets into files on the repo-server, and carefully limiting who can `create` or `update` Applications.	6.8	More Details
CVE-2021-25220	BIND 9.11.0 -> 9.11.36 9.12.0 -> 9.16.26 9.17.0 -> 9.18.0 BIND Supported Preview Editions: 9.11.4-S1 -> 9.11.36-S1 9.16.8-S1 -> 9.16.26-S1 Versions of BIND 9 earlier than those shown - back to 9.1.0, including Supported Preview Editions - are also believed to be affected but have not been tested as they are EOL. The cache could become poisoned with incorrect records leading to queries being made to the wrong servers, which might also result in false information being returned to clients.	6.8	More Details
CVE-2022-22948	The vCenter Server contains an information disclosure vulnerability due to improper permission of files. A malicious actor with non-administrative access to the vCenter Server may exploit this issue to gain access to sensitive information.	6.5	More Details
CVE-2022-26280	Libarchive v3.6.0 was discovered to contain an out-of-bounds read via the component zipx_lzma_alone_init.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26252	aaPanel v6.8.21 was discovered to be vulnerable to directory traversal. This vulnerability allows attackers to obtain the root user private SSH key(id_rsa).	6.5	More Details
CVE-2022-24956	An issue was discovered in Shopware B2B-Suite through 4.4.1. The sort-by parameter of the search functionality of b2border and b2borderlist allows SQL injection. Possible techniques are boolean-based blind, time-based blind, and potentially stacked queries. The vulnerability allows a remote authenticated attacker to dump the underlying database.	6.5	More Details
CVE-2022-0549	An issue has been discovered in GitLab CE/EE affecting all versions before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. Under certain conditions, GitLab REST API may allow unprivileged users to add other users to groups even if that is not possible to do through the Web UI.	6.5	More Details
CVE-2022-0751	Inaccurate display of Snippet files containing special characters in all versions of GitLab CE/EE allows an attacker to create Snippets with misleading content which could trick unsuspecting users into executing arbitrary commands	6.5	More Details
CVE-2021-43737	An issus was discovered in xiaohuanxiong CMS 5.0.17. There is a CSRF vulnerability that can modify administrator account's password.	6.5	More Details
CVE-2022-22316	IBM MQ Appliance 9.2 CD and 9.2 LTS could allow an authenticated and authorized user to cause a denial of service due to incorrectly configured authorization checks. IBM X-Force ID: 218276.	6.5	More Details
CVE-2022-28158	A missing permission check in Jenkins Pipeline: Phoenix AutoTest Plugin 1.3 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	6.5	More Details
CVE-2022-25590	SurveyKing v0.2.0 was discovered to retain users' session cookies after logout, allowing attackers to login to the system and access data using the browser cache when the user exits the application.	6.5	More Details
CVE-2022-28143	A cross-site request forgery (CSRF) vulnerability in Jenkins Proxmox Plugin 0.7.0 and earlier allows attackers to connect to an attacker-specified host using attacker-specified username and password (perform a connection test), disable SSL/TLS validation for the entire Jenkins controller JVM as part of the connection test (see CVE-2022-28142), and test a rollback with attacker-specified parameters.	6.5	More Details
CVE-2022-28160	Jenkins Tests Selector Plugin 1.3.3 and earlier allows users with Item/Configure permission to read arbitrary files on the Jenkins controller.	6.5	More Details
CVE-2022-28157	Jenkins Pipeline: Phoenix AutoTest Plugin 1.3 and earlier allows attackers with Item/Configure permission to upload arbitrary files from the Jenkins controller via FTP to an attacker-specified FTP server.	6.5	More Details
CVE-2022-28156	Jenkins Pipeline: Phoenix AutoTest Plugin 1.3 and earlier allows attackers with Item/Configure permission to copy arbitrary files and directories from the Jenkins controller to the agent workspace.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0859	McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a local attacker to point an ePO server to an arbitrary SQL server during the restoration of the ePO server. To achieve this the attacker would have to be logged onto the server hosting the ePO server (restricted to administrators) and to know the SQL server password.	6.5	More Details
CVE-2022-28148	The file browser in Jenkins Continuous Integration with Toad Edge Plugin 2.3 and earlier may interpret some paths to files as absolute on Windows, resulting in a path traversal vulnerability allowing attackers with Item/Read permission to obtain the contents of arbitrary files on Windows controllers.	6.5	More Details
CVE-2022-0996	A vulnerability was found in the 389 Directory Server that allows expired passwords to access the database to cause improper authentication.	6.5	More Details
CVE-2022-28146	Jenkins Continuous Integration with Toad Edge Plugin 2.3 and earlier allows attackers with Item/Configure permission to read arbitrary files on the Jenkins controller by specifying an input folder on the Jenkins controller as a parameter to its build steps.	6.5	More Details
CVE-2021-3582	A flaw was found in the QEMU implementation of VMWare's paravirtual RDMA device. The issue occurs while handling a "PVRDMA_CMD_CREATE_MR" command due to improper memory remapping (mremap). This flaw allows a malicious guest to crash the QEMU process on the host. The highest threat from this vulnerability is to system availability.	6.5	More Details
CVE-2022-28144	Jenkins Proxmox Plugin 0.7.0 and earlier does not perform a permission check in several HTTP endpoints, allowing attackers with Overall/Read permission to connect to an attacker-specified host using attacker-specified username and password (perform a connection test), disable SSL/TLS validation for the entire Jenkins controller JVM as part of the connection test (see CVE-2022-28142), and test a rollback with attacker-specified parameters.	6.5	More Details
CVE-2021-3941	In ImfChromaticities.cpp routine RGBtoXYZ(), there are some division operations such as `float Z = (1 - chroma.white.x - chroma.white.y) * Y / chroma.white.y;` and `chroma.green.y * (X + Z))) / d;` but the divisor is not checked for a 0 value. A specially crafted file could trigger a divide-by-zero condition which could affect the availability of programs linked with OpenEXR.	6.5	More Details
CVE-2020-20093	The Facebook Messenger app for iOS 227.0 and prior and Android 228.1.0.10.116 and prior user interface does not properly represent URI messages to the user, which results in URI spoofing via specially crafted messages.	6.5	More Details
CVE-2021-43701	CSZ CMS 1.2.9 has a Time and Boolean-based Blind SQL Injection vulnerability in the endpoint /admin/export/getcsv/article_db, via the fieldS[] and orderby parameters.	6.5	More Details
CVE-2022-28141	Jenkins Proxmox Plugin 0.5.0 and earlier stores the Proxmox Datacenter password unencrypted in the global config.xml file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2021-4147	A flaw was found in the libvirt libxl driver. A malicious guest could continuously reboot itself and cause libvirtd on the host to deadlock or crash, resulting in a denial of service condition.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28135	Jenkins instant-messaging Plugin 1.41 and earlier stores passwords for group chats unencrypted in the global configuration file of plugins based on Jenkins instant-messaging Plugin on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2021-45491	3CX System through 2022-03-17 stores cleartext passwords in a database.	6.5	More Details
CVE-2020-20096	Whatsapp iOS 2.19.80 and prior and Android 2.19.222 and prior user interface does not properly represent URI messages to the user, which results in URI spoofing via specially crafted messages.	6.5	More Details
CVE-2020-20094	Instagram iOS 106.0 and prior and Android 107.0.0.11 and prior user interface does not properly represent URI messages to the user, which results in URI spoofing via specially crafted messages	6.5	More Details
CVE-2020-20095	iMessage (Messages app) iOS 12.4 and prior user interface does not properly represent URI messages to the user, which results in URI spoofing via specially crafted messages.	6.5	More Details
CVE-2022-0750	The Photoswipe Masonry Gallery WordPress plugin is vulnerable to Cross-Site Scripting due to insufficient escaping and sanitization of the thumbnail_width, thumbnail_height, max_image_width, and max_image_height parameters found in the ~/photoswipe-masonry.php file which allows authenticated attackers to inject arbitrary web scripts into galleries created by the plugin and on the PhotoSwipe Options page. This affects versions up to and including 1.2.14.	6.4	More Details
CVE-2022-21820	NVIDIA DCGM contains a vulnerability in nvhostengine, where a network user can cause detection of error conditions without action, which may lead to limited code execution, some denial of service, escalation of privileges, and limited impacts to both data confidentiality and integrity.	6.3	More Details
CVE-2022-23242	TeamViewer Linux versions before 15.28 do not properly execute a deletion command for the connection password in case of a process crash. Knowledge of the crash event and the TeamViewer ID as well as either possession of the pre-crash connection password or local authenticated access to the machine would have allowed to establish a remote connection by reusing the not properly deleted connection password.	6.3	More Details
CVE-2021-43725	There is a Cross Site Scripting (XSS) vulnerability in SpotPage_login.php of Spotweb 1.5.1 and below, which allows remote attackers to inject arbitrary web script or HTML via the data[performredirect] parameter.	6.1	More Details
CVE-2021-25071	The WordPress plugin through 2.0.1 does not sanitise and escape the translation parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-0599	The Mapping Multiple URLs Redirect Same Page WordPress plugin through 5.8 does not sanitize and escape the mmursp_id parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43721	Leanote 2.7.0 is vulnerable to Cross Site Scripting (XSS) in the markdown type note. This leads to remote code execution with payload : <video src=x onerror=(function() {require('child_process').exec('calc');})();>	6.1	More Details
CVE-2021-25012	The Pz-LinkCard WordPress plugin through 2.4.4.4 does not sanitise and escape multiple parameters before outputting them back in admin dashboard pages, leading to Reflected Cross-Site Scripting issues	6.1	More Details
CVE-2022-0641	The Popup Like box WordPress plugin before 3.6.1 does not sanitize and escape the ays_fb_tab parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-0600	The Conference Scheduler WordPress plugin before 2.4.3 does not sanitize and escape the tab parameter before outputting back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-0619	The Database Peek WordPress plugin through 1.2 does not sanitize and escape the match parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-0620	The Delete Old Orders WordPress plugin through 0.2 does not sanitize and escape the date parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-0621	The dTabs WordPress plugin through 1.4 does not sanitize and escape the tab parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-25575	Multiple cross-site scripting (XSS) vulnerabilities in Parking Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via crafted payloads injected into the user name, password, and verification code text boxes.	6.1	More Details
CVE-2022-0643	The Bank Mellat WordPress plugin through 1.3.7 does not sanitize and escape the orderId parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-0647	The Bulk Creator WordPress plugin through 1.0.1 does not sanitize and escape the post_type parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-0680	The Plezi WordPress plugin before 1.0.3 has a REST endpoint allowing unauthenticated users to update the plz_configuration_tracker_enable option, which is then displayed in the admin panel without sanitisation and escaping, leading to a Stored Cross-Site Scripting issue	6.1	More Details
CVE-2022-0818	The WooCommerce Affiliate Plugin WordPress plugin before 4.16.4.5 does not have authorization and CSRF checks on a specific action handler, as well as does not sanitize its settings, which enables an unauthenticated attacker to inject malicious XSS payloads into the settings page of the plugin.	6.1	More Details
CVE-2022-26980	Teampass 2.1.26 allows reflected XSS via the index.php PATH_INFO.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44212	OX App Suite through 7.10.5 allows XSS via a trailing control character such as the SCRIPT\t substring.	6.1	More Details
CVE-2021-42970	Cross Site Scripting (XSS) vulnerability exists in cxuucms v3 via the imgurl of /feedback/post/ content parameter.	6.1	More Details
CVE-2021-44213	OX App Suite through 7.10.5 allows XSS via uuencoding in a multipart/alternative message.	6.1	More Details
CVE-2021-24746	The Social Sharing Plugin WordPress plugin before 3.3.40 does not escape the viewed post URL before outputting it back in onclick attributes when the "Enable 'More' icon" option is enabled (which is the default setting), leading to a Reflected Cross-Site Scripting issue.	6.1	More Details
CVE-2022-26263	Yonyou u8 v13.0 was discovered to contain a DOM-based cross-site scripting (XSS) vulnerability via the component /u8sl/WebHelp.	6.1	More Details
CVE-2021-27473	Rockwell Automation Connected Components Workbench v12.00.00 and prior does not sanitize paths specified within the .ccwarc archive file during extraction. This type of vulnerability is also commonly referred to as a Zip Slip. A local, authenticated attacker can create a malicious .ccwarc archive file that, when opened by Connected Components Workbench, will allow the attacker to gain the privileges of the software. If the software is running at SYSTEM level, the attacker will gain admin level privileges. User interaction is required for this exploit to be successful.	6.1	More Details
CVE-2022-26573	Maccms v10 was discovered to contain multiple reflected cross-site scripting (XSS) vulnerabilities in /admin.php/admin/art/data.html via the select and input parameters.	6.1	More Details
CVE-2022-1058	Open Redirect on login in GitHub repository go-gitea/gitea prior to 1.16.5.	6.1	More Details
CVE-2022-27885	Maccms v10 was discovered to contain multiple reflected cross-site scripting (XSS) vulnerabilities in /admin.php/admin/website/data.html via the select and input parameters.	6.1	More Details
CVE-2021-44768	Delta Electronics CNCSoft (Version 1.01.30) and prior) is vulnerable to an out-of-bounds read while processing a specific project file, which may allow an attacker to disclose information.	6.1	More Details
CVE-2021-20323	A POST based reflected Cross Site Scripting vulnerability on has been identified in Keycloak.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20290	An improper authorization handling flaw was found in Foreman. The OpenSCAP plugin for the smart-proxy allows foreman clients to execute actions that should be limited to the Foreman Server. This flaw allows an authenticated local attacker to access and delete limited resources and also causes a denial of service on the Foreman server. The highest threat from this vulnerability is to integrity and system availability.	6.1	More Details
CVE-2021-40906	CheckMK Raw Edition software (versions 1.5.0 to 1.6.0) does not sanitise the input of a web service parameter that is in an unauthenticated zone. This Reflected XSS allows an attacker to open a backdoor on the device with HTML content and interpreted by the browser (such as JavaScript or other client-side scripts) or to steal the session cookies of a user who has previously authenticated via a man in the middle. Successful exploitation requires access to the web service resource without authentication.	6.1	More Details
CVE-2022-25269	Passwork On-Premise Edition before 4.6.13 has multiple XSS issues.	6.1	More Details
CVE-2021-44208	OX App Suite through 7.10.5 allows XSS via an unknown system message in Chat.	6.1	More Details
CVE-2022-27886	Maccms v10 was discovered to contain a reflected cross-site scripting (XSS) vulnerability in /admin.php/admin/ulog/index.html via the wd parameter.	6.1	More Details
CVE-2022-27887	Maccms v10 was discovered to contain a reflected cross-site scripting (XSS) vulnerability in /admin.php/admin/vod/data.html via the repeat parameter.	6.1	More Details
CVE-2021-46426	phpIPAM 1.4.4 allows Reflected XSS and CSRF via app/admin/subnets/find_free_section_subnets.php of the subnets functionality.	6.1	More Details
CVE-2022-24776	Flask-AppBuilder is an application development framework, built on top of the Flask web framework. Flask-AppBuilder contains an open redirect vulnerability when using database authentication login page on versions below 3.4.5. This issue is fixed in version 3.4.5. There are currently no known workarounds.	6.1	More Details
CVE-2022-25221	Money Transfer Management System Version 1.0 allows an attacker to inject JavaScript code in the URL and then trick a user into visit the link in order to execute JavaScript code.	6.1	More Details
CVE-2021-44209	OX App Suite through 7.10.5 allows XSS via an HTML 5 element such as AUDIO.	6.1	More Details
CVE-2021-44210	OX App Suite through 7.10.5 allows XSS via NIFF (Notation Interchange File Format) data.	6.1	More Details
CVE-2022-27920	libkiwix 10.0.0 and 10.0.1 allows XSS in the built-in webserver functionality via the search suggestions URL parameter. This is fixed in 10.1.0.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27884	Maccms v10 was discovered to contain a reflected cross-site scripting (XSS) vulnerability in /admin.php/admin/plog/index.html via the wd parameter.	6.1	More Details
CVE-2022-27906	Mendelson OFTP2 before 1.1 b43 is affected by directory traversal. To access the vulnerable code path, the attacker has to know one of the configured Odette IDs of the OFTP2 server. An attacker can upload files to the server outside of the intended upload directory.	5.9	More Details
CVE-2022-24769	Moby is an open-source project created by Docker to enable and accelerate software containerization. A bug was found in Moby (Docker Engine) prior to version 20.10.14 where containers were incorrectly started with non-empty inheritable Linux process capabilities, creating an atypical Linux environment and enabling programs with inheritable file capabilities to elevate those capabilities to the permitted set during `execve(2)`. Normally, when executable programs have specified permitted file capabilities, otherwise unprivileged users and processes can execute those programs and gain the specified file capabilities up to the bounding set. Due to this bug, containers which included executable programs with inheritable file capabilities allowed otherwise unprivileged users and processes to additionally gain these inheritable file capabilities up to the container's bounding set. Containers which use Linux users and groups to perform privilege separation inside the container are most directly impacted. This bug did not affect the container security sandbox as the inheritable set never contained more capabilities than were included in the container's bounding set. This bug has been fixed in Moby (Docker Engine) 20.10.14. Running containers should be stopped, deleted, and recreated for the inheritable capabilities to be reset. This fix changes Moby (Docker Engine) behavior such that containers are started with a more typical Linux environment. As a workaround, the entry point of a container can be modified to use a utility like `capsh(1)` to drop inheritable capabilities prior to the primary process starting.	5.9	More Details
CVE-2022-0123	An issue has been discovered affecting GitLab versions prior to 14.4.5, between 14.5.0 and 14.5.3, and between 14.6.0 and 14.6.1. GitLab does not validate SSL certificates for some of external CI services which makes it possible to perform MitM attacks on connections to these external services.	5.9	More Details
CVE-2021-4150	A use-after-free flaw was found in the add_partition in block/partitions/core.c in the Linux kernel. A local attacker with user privileges could cause a denial of service on the system. The issue results from the lack of code cleanup when device_add call fails when adding a partition to the disk.	5.5	More Details
CVE-2021-4149	A vulnerability was found in btrfs_alloc_tree_b in fs/btrfs/extent-tree.c in the Linux kernel due to an improper lock operation in btrfs. In this flaw, a user with a local privilege may cause a denial of service (DOS) due to a deadlock problem.	5.5	More Details
CVE-2022-26296	BOOM: The Berkeley Out-of-Order RISC-V Processor commit d77c2c3 was discovered to allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.	5.5	More Details
CVE-2022-26291	lrzip v0.641 was discovered to contain a multiple concurrency use-after-free between the functions zpaq_decompress_buf() and clear_rulist(). This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted lrz file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1056	Out-of-bounds Read error in tiffcrop in libtiff 4.3.0 allows attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 46dc8fcd.	5.5	More Details
CVE-2022-1052	Heap Buffer Overflow in iterate_chained_fixups in GitHub repository radareorg/radare2 prior to 5.6.6.	5.5	More Details
CVE-2021-28275	A Denial of Service vulnerability exists in jhead 3.04 and 3.05 due to a wild address read in the Get16u function in exif.c in will cause segmentation fault via a crafted_file.	5.5	More Details
CVE-2008-10001	A vulnerability, which was classified as problematic, has been found in Pro2col Stingray FTS. The manipulation of the argument Username leads to cross site scripting. The attack may be initiated remotely. It is recommended to upgrade the affected component. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	5.5	More Details
CVE-2021-4219	A flaw was found in ImageMagick. The vulnerability occurs due to improper use of open functions and leads to a denial of service. This flaw allows an attacker to crash the system.	5.5	More Details
CVE-2022-27939	tcprewrite in Tcpreplay 4.4.1 has a reachable assertion in get_layer4_v6 in common/get.c.	5.5	More Details
CVE-2021-3933	An integer overflow could occur when OpenEXR processes a crafted file on systems where size_t < 64 bits. This could cause an invalid bytesPerLine and maxBytesPerLine value, which could lead to problems with application stability or lead to other attack paths.	5.5	More Details
CVE-2022-27943	libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	5.5	More Details
CVE-2022-27950	In drivers/hid/hid-elo.c in the Linux kernel before 5.16.11, a memory leak exists for a certain hid_parse error condition.	5.5	More Details
CVE-2022-1122	A flaw was found in the opj2_decompress program in openjpeg2 2.4.0 in the way it handles an input directory with a large number of files. When it fails to allocate a buffer to store the filenames of the input directory, it calls free() on an uninitialized pointer, leading to a segmentation fault and a denial of service.	5.5	More Details
CVE-2021-22572	On unix-like systems, the system temporary directory is shared between all users on that system. The root cause is File.createTempFile creates files in the the system temporary directory with world readable permissions. Any sensitive information written to theses files is visible to all other local users on unix-like systems. We recommend upgrading past commit https://github.com/google/data-transfer-project/pull/969	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0854	A memory leak flaw was found in the Linux kernel's DMA subsystem, in the way a user calls DMA_FROM_DEVICE. This flaw allows a local user to read random memory from the kernel space.	5.5	More Details
CVE-2021-4148	A vulnerability was found in the Linux kernel's block_invalidatepage in fs/buffer.c in the filesystem. A missing sanity check may allow a local attacker with user privilege to cause a denial of service (DOS) problem.	5.5	More Details
CVE-2022-0322	A flaw was found in the sctp_make_strreset_req function in net/sctp/sm_make_chunk.c in the SCTP network protocol in the Linux kernel with a local user privilege access. In this flaw, an attempt to use more buffer than is allocated triggers a BUG_ON issue, leading to a denial of service (DOS).	5.5	More Details
CVE-2022-27938	stb_image.h (aka the stb image loader) 2.19, as used in libsixel and other products, has a reachable assertion in stbi__create_png_image_raw.	5.5	More Details
CVE-2021-39491	A Cross Site Scripting (XSS) vulnerability exists in Yogesh Ojha reNgine v1.0 via the Scan Engine name file in the Scan Engine deletion confirmation modal box . .	5.4	More Details
CVE-2022-0857	A reflected cross-site scripting (XSS) vulnerability in McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote attacker to potentially obtain access to an ePO administrator's session by convincing the attacker to click on a carefully crafted link. This would lead to limited access to sensitive information and limited ability to alter some information in ePO due to the area of the User Interface the vulnerability is present in.	5.4	More Details
CVE-2022-23903	A Cross Site Scripting (XSS) vulnerability exists in pearadmin pear-admin-think <=5.0.6, which allows a login account to access arbitrary functions and cause stored XSS through a fake User-Agent.	5.4	More Details
CVE-2022-0842	A blind SQL injection vulnerability in McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote authenticated attacker to potentially obtain information from the ePO database. The data obtained is dependent on the privileges the attacker has and to obtain sensitive data the attacker would require administrator privileges.	5.4	More Details
CVE-2021-43659	In halo 1.4.14, the function point of uploading the avatar, any file can be uploaded, such as uploading an HTML file, which will cause a stored XSS vulnerability.	5.4	More Details
CVE-2022-25582	A stored cross-site scripting (XSS) vulnerability in the Column module of ClassCMS v2.5 and below allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Add Articles field.	5.4	More Details
CVE-2022-28159	Jenkins Tests Selector Plugin 1.3.3 and earlier does not escape the Properties File Path option for Choosing Tests parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-28153	Jenkins SiteMonitor Plugin 0.6 and earlier does not escape URLs of sites to monitor in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24957	DHC Vision eQMS through 5.4.8.322 has Persistent XSS due to insufficient encoding of untrusted input/output. To exploit the vulnerability, the attacker has to create or edit a new information object and use the XSS payload as the name. Any user that opens the object's version or history tab will be attacked.	5.4	More Details
CVE-2022-28149	Jenkins Job and Node ownership Plugin 0.13.0 and earlier does not escape the names of the secondary owners, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-28145	Jenkins Continuous Integration with Toad Edge Plugin 2.3 and earlier does not apply Content-Security-Policy headers to report files it serves, resulting in a stored cross-site scripting (XSS) exploitable by attackers with Item/Configure permission or otherwise able to control report contents.	5.4	More Details
CVE-2021-44211	OX App Suite through 7.10.5 allows XSS via the class attribute of an element in an HTML e-mail signature.	5.4	More Details
CVE-2022-28133	Jenkins Bitbucket Server Integration Plugin 3.1.0 and earlier does not limit URL schemes for callback URLs on OAuth consumers, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to create BitBucket Server consumers.	5.4	More Details
CVE-2022-24643	A stored cross-site scripting (XSS) issue was discovered in the OpenEMR Hospital Information Management System version 6.0.0.	5.4	More Details
CVE-2021-45866	A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Student Attendance Management System 1.0 via the couse filed in index.php.	5.4	More Details
CVE-2022-28134	Jenkins Bitbucket Server Integration Plugin 3.1.0 and earlier does not perform permission checks in several HTTP endpoints, allowing attackers with Overall/Read permission to create, view, and delete BitBucket Server consumers.	5.4	More Details
CVE-2022-25608	Cross-Site Request Forgery (CSRF) in Yoo Slider – Image Slider & Video Slider (WordPress plugin) allows attackers to trick authenticated users into unwanted slider duplicate or delete action.	5.4	More Details
CVE-2022-0720	The Amelia WordPress plugin before 1.0.47 does not have proper authorisation when managing appointments, allowing any customer to update other's booking, as well as retrieve sensitive information about the bookings, such as the full name and phone number of the person who booked it.	5.4	More Details
CVE-2005-10001	A vulnerability was found in Netegrity SiteMinder up to 4.5.1 and classified as critical. Affected by this issue is the file /siteminderagent/pwcgi/smpwservicescgi.exe of the component Login. The manipulation of the argument target leads to an open redirect. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	5.4	More Details
CVE-2022-0595	The Drag and Drop Multiple File Upload WordPress plugin before 1.3.6.3 allows SVG files to be uploaded by default via the dnd_codedropz_upload AJAX action, which could lead to Stored Cross-Site Scripting issue	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0450	The Menu Image, Icons made easy WordPress plugin before 3.0.6 does not have authorisation and CSRF checks when saving menu settings, and does not validate, sanitise and escape them. As a result, any authenticate users, such as subscriber can update the settings or arbitrary menu and put Cross-Site Scripting payloads in them which will be triggered in the related menu in the frontend	5.4	More Details
CVE-2022-0397	The WPC Smart Wishlist for WooCommerce WordPress plugin before 2.9.4 does not sanitise and escape the key parameter before outputting it back in the wishlist_quickview AJAX action's response (available to any authenticated user), leading to a Reflected Cross-Site Scripting	5.4	More Details
CVE-2022-26197	Joget DX 7 was discovered to contain a cross-site scripting (XSS) vulnerability via the Datalist table.	5.4	More Details
CVE-2022-25609	Stored Cross-Site Scripting (XSS) in Yoo Slider – Image Slider & Video Slider (WordPress plugin) allows attackers with contributor or higher user role to inject the malicious code.	5.4	More Details
CVE-2022-0136	A vulnerability was discovered in GitLab versions 10.5 to 14.5.4, 14.6 to 14.6.4, and 14.7 to 14.7.1. GitLab was vulnerable to a blind SSRF attack through the Project Import feature.	5.4	More Details
CVE-2022-0145	Cross-site Scripting (XSS) - Stored in GitHub repository forkcms/forkcms prior to 5.11.1.	5.4	More Details
CVE-2022-27254	The remote keyless system on Honda Civic 2018 vehicles sends the same RF signal for each door-open request, which allows for a replay attack, a related issue to CVE-2019-20626.	5.3	More Details
CVE-2021-4191	An issue has been discovered in GitLab CE/EE affecting versions 13.0 to 14.6.5, 14.7 to 14.7.4, and 14.8 to 14.8.2. Private GitLab instances with restricted sign-ups may be vulnerable to user enumeration to unauthenticated users through the GraphQL API.	5.3	More Details
CVE-2022-23937	In Wind River VxWorks 6.9 and 7, a specific crafted packet may lead to an out-of-bounds read during an IKE initial exchange scenario.	5.3	More Details
CVE-2021-27418	GE UR firmware versions prior to version 8.1x supports web interface with read-only access. The device fails to properly validate user input, making it possible to perform cross-site scripting attacks, which may be used to send a malicious script. Also, UR Firmware web server does not perform HTML encoding of user-supplied strings.	5.3	More Details
CVE-2022-0331	An information disclosure vulnerability in Webadmin allows an unauthenticated remote attacker to read the device serial number in Sophos Firewall version v18.5 MR2 and older.	5.3	More Details
CVE-2021-46434	EMQ X Dashboard V3.0.0 is affected by username enumeration in the "/api /v3/auth" interface. When a user login, the application returns different results depending on whether the account is correct, that allowed an attacker to determine if a given username was valid	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26254	WoWonder The Ultimate PHP Social Network Platform v4.0.0 was discovered to contain an access control issue which allows unauthenticated attackers to arbitrarily change group ID names.	5.3	More Details
CVE-2021-26598	ImpressCMS before 1.4.3 has Incorrect Access Control because include/findusers.php allows access by unauthenticated attackers (who are, by design, able to have a security token).	5.3	More Details
CVE-2021-24978	The OSMapper WordPress plugin through 2.1.5 contains an AJAX action to delete a plugin related post type named 'map' and is registered with the wp_ajax_nopriv prefix, making it available to unauthenticated users. There is no authorisation, CSRF and checks in place to ensure that the post to delete is a map one. As a result, unauthenticated user can delete arbitrary posts from the blog	5.3	More Details
CVE-2021-22100	In cloud foundry CAPI versions prior to 1.122, a denial-of-service attack in which a developer can push a service broker that (accidentally or maliciously) causes CC instances to timeout and fail is possible. An attacker can leverage this vulnerability to cause an inability for anyone to push or manage apps.	5.3	More Details
CVE-2022-1077	A vulnerability was found in TEM FLEX-1080 and FLEX-1085 1.6.0. It has been declared as problematic. This vulnerability log.cgi of the component Log Handler. A direct request leads to information disclosure of hardware information. The attack can be initiated remotely and does not require any form of authentication.	5.3	More Details
CVE-2021-27420	GE UR firmware versions prior to version 8.1x web server task does not properly handle receipt of unsupported HTTP verbs, resulting in the web server becoming temporarily unresponsive after receiving a series of unsupported HTTP requests. When unresponsive, the web server is inaccessible. By itself, this is not particularly significant as the relay remains effective in all other functionality and communication channels.	5.3	More Details
CVE-2015-10002	A vulnerability classified as problematic has been found in Kiddoware Kids Place. This affects the Home Button Protection. A repeated pressing of the button causes a local denial of service. It is recommended to upgrade the affected component.	5.3	More Details
CVE-2021-27424	GE UR firmware versions prior to version 8.1x shares MODBUS memory map as part of the communications guide. GE was made aware a “Last-key pressed” MODBUS register can be used to gain unauthorized information.	5.3	More Details
CVE-2010-10001	A vulnerability, which was classified as problematic, was found in Shemes GrabIt up to 1.7.2 Beta 4. This affects the component NZB Date Parser. The manipulation of the argument date with the input 1000000000000000 as part of a NZB File leads to a denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2003-5001	A vulnerability was found in ISS BlackICE PC Protection and classified as critical. Affected by this issue is the component Cross Site Scripting Detection. The manipulation as part of POST/PUT/DELETE/OPTIONS Request leads to privilege escalation. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0396	BIND 9.16.11 -> 9.16.26, 9.17.0 -> 9.18.0 and versions 9.16.11-S1 -> 9.16.26-S1 of the BIND Supported Preview Edition. Specifically crafted TCP streams can cause connections to BIND to remain in CLOSE_WAIT status for an indefinite period of time, even after the client has terminated the connection.	5.3	More Details
CVE-2003-5003	A vulnerability was found in ISS BlackICE PC Protection. It has been rated as problematic. Affected by this issue is the Update Handler. The manipulation with an unknown input leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	5.0	More Details
CVE-2022-0493	The String locator WordPress plugin before 2.5.0 does not properly validate the path of the files to be searched, allowing high privilege users such as admin to query arbitrary files on the web server via a path traversal vector. Furthermore, due to a flaw in the search, allowing a pattern to be provided, which will be used to output the relevant matches from the matching file, all content of the file can be disclosed.	4.9	More Details
CVE-2021-43099	An Archive Extraction (AKA "Zip Slip) vulnerability exists in bbs 5.3 in the UpgradeNow function in UpgradeManageAction.java, which unzips the arbitrary upladed zip file without checking filenames. The vulnerability is exploited using a specially crafted archive that holds directory traversal filenames (e.g. ../../evil.exe).	4.9	More Details
CVE-2022-23059	A Stored Cross Site Scripting (XSS) vulnerability exists in Shopizer versions 2.0 through 2.17.0 via the “Manage Images” tab, which allows an attacker to upload a SVG file containing malicious JavaScript code.	4.8	More Details
CVE-2022-0955	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/data-hub prior to 1.2.4.	4.8	More Details
CVE-2022-25606	Multiple Authenticated Stored Cross-Site Scripting (XSS) vulnerabilities discovered in WP-DownloadManager WordPress plugin (versions <= 1.68.6). Vulnerable parameters &download_path, &download_path_url, &download_page_url, &download_categories.	4.8	More Details
CVE-2022-25574	A stored cross-site scripting (XSS) vulnerability in the upload function of /admin/show.php allows attackers to execute arbitrary web scripts or HTML via a crafted image file.	4.8	More Details
CVE-2022-0388	The Interactive Medical Drawing of Human Body WordPress plugin before 2.6 does not sanitise and escape the Link field, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-0283	An issue has been discovered affecting GitLab versions prior to 13.5. An open redirect vulnerability was fixed in GitLab integration with Jira that a could cause the web application to redirect the request to the attacker specified URL.	4.7	More Details
CVE-2022-26269	Suzuki Connect v1.0.15 allows attackers to tamper with displayed messages via spoofed CAN messages.	4.6	More Details
CVE-2022-25576	Anchor CMS v0.12.7 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component anchor/routes/posts.php. This vulnerability allows attackers to arbitrarily delete posts.	4.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0494	A kernel information leak flaw was identified in the scsi_ioctl function in drivers/scsi/scsi_ioctl.c in the Linux kernel. This flaw allows a local attacker with a special user privilege (CAP_SYS_ADMIN or CAP_SYS_RAWIO) to create issues with confidentiality.	4.4	More Details
CVE-2022-28151	A missing permission check in Jenkins Job and Node ownership Plugin 0.13.0 and earlier allows attackers with Item/Read permission to change the owners and item-specific permissions of a job.	4.3	More Details
CVE-2022-28147	A missing permission check in Jenkins Continuous Integration with Toad Edge Plugin 2.3 and earlier allows attackers with Overall/Read permission to check for the existence of an attacker-specified file path on the Jenkins controller file system.	4.3	More Details
CVE-2022-28152	A cross-site request forgery (CSRF) vulnerability in Jenkins Job and Node ownership Plugin 0.13.0 and earlier allows attackers to restore the default ownership of a job.	4.3	More Details
CVE-2022-0858	A cross-site scripting (XSS) vulnerability in McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote attacker to potentially obtain access to an ePO administrator's session by convincing the attacker to click on a carefully crafted link. This would lead to limited ability to alter some information in ePO due to the area of the User Interface the vulnerability is present in.	4.3	More Details
CVE-2022-28137	A missing permission check in Jenkins JiraTestResultReporter Plugin 165.v817928553942 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials.	4.3	More Details
CVE-2022-25266	Passwork On-Premise Edition before 4.6.13 allows migration/downloadExportFile Directory Traversal (to read files).	4.3	More Details
CVE-2021-44751	A vulnerability affecting F-Secure SAFE browser was discovered. A maliciously crafted website attached with USSD code in JavaScript or iFrame can trigger dialer application from F-Secure browser which can be exploited by an attacker to send unwanted USSD messages or perform unwanted calls. In most modern Android OS, dialer application will require user interaction, however, some older Android OS may not need user interaction.	4.3	More Details
CVE-2022-28139	A missing permission check in Jenkins RocketChat Notifier Plugin 1.4.10 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials.	4.3	More Details
CVE-2022-25223	Money Transfer Management System Version 1.0 allows an authenticated user to inject SQL queries in 'mtms/admin/?page=transaction/view_details' via the 'id' parameter.	4.3	More Details
CVE-2022-28138	A cross-site request forgery (CSRF) vulnerability in Jenkins RocketChat Notifier Plugin 1.4.10 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credential.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0833	The Church Admin WordPress plugin before 3.4.135 does not have authorisation and CSRF in some of its action as well as requested files, allowing unauthenticated attackers to repeatedly request the "refresh-backup" action, and simultaneously keep requesting a publicly accessible temporary file generated by the plugin in order to disclose the final backup filename, which can then be fetched by the attacker to download the backup of the plugin's DB data	4.3	More Details
CVE-2022-24782	Discourse is an open source discussion platform. Versions 2.8.2 and prior in the `stable` branch, 2.9.0.beta3 and prior in the `beta` branch, and 2.9.0.beta3 and prior in the `tests-passed` branch are vulnerable to a data leak. Users can request an export of their own activity. Sometimes, due to category settings, they may have category membership for a secure category. The name of this secure category is shown to the user in the export. The same thing occurs when the user's post has been moved to a secure category. A patch for this issue is available in the `main` branch of Discourse's GitHub repository and is anticipated to be part of future releases.	4.3	More Details
CVE-2022-25041	OpenEMR v6.0.0 was discovered to contain an incorrect access control issue.	4.3	More Details
CVE-2021-4180	An information exposure flaw in openstack-tripleo-heat-templates allows an external user to discover the internal IP or hostname. An attacker could exploit this by checking the www_authenticate_uri parameter (which is visible to all end users) in configuration files. This would give sensitive information which may aid in additional system exploitation. This flaw affects openstack-tripleo-heat-templates versions prior to 11.6.1.	4.3	More Details
CVE-2021-43105	A vulnerability in the bailiwick checking function in Technitium DNS Server <= v7.0 exists that allows specific malicious users to inject `NS` records of any domain (even TLDs) into the cache and conduct a DNS cache poisoning attack.	4.3	More Details
CVE-2022-1074	A vulnerability has been found in TEM FLEX-1085 1.6.0 and classified as problematic. Using the input HTML Injection in the WiFi settings of the dashboard leads to html injection.	4.3	More Details
CVE-2022-1076	A vulnerability was found in Automatic Question Paper Generator System 1.0. It has been classified as problematic. This affects the file /aqpg/users/login.php of the component My Account Page. The manipulation of the argument First Name/Middle Name/Last Name leads to cross site scripting. It is possible to initiate the attack remotely.	4.3	More Details
CVE-2022-1079	A vulnerability classified as problematic has been found in SourceCodester One Church Management System. Affected are multiple files and parameters which are prone to to cross site scripting. It is possible to launch the attack remotely.	4.3	More Details
CVE-2022-0371	An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.4 before 14.5.4, all versions starting from 14.6 before 14.6.4, all versions starting from 14.7 before 14.7.1. GitLab search may allow authenticated users to search other users by their respective private emails even if a user set their email to private.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1081	A vulnerability was found in SourceCodester Microfinance Management System 1.0. It has been declared as problematic. This vulnerability affects the file /mims/app/addcustomerHandler.php. The manipulation of the argument first_name, middle_name, and surname leads to cross site scripting. The attack can be initiated remotely.	4.3	More Details
CVE-2022-0897	A flaw was found in the libvirt nwfilter driver. The virNWFilterObjListNumOfNWFilters method failed to acquire the driver->nwfilters mutex before iterating over virNWFilterObj instances. There was no protection to stop another thread from concurrently modifying the driver->nwfilters object. This flaw allows a malicious, unprivileged user to exploit this issue via libvirt's API virConnectNumOfNWFilters to crash the network filter management daemon (libvirtd/virtnwfilterd).	4.3	More Details
CVE-2021-39876	In all versions of GitLab CE/EE since version 11.3, the endpoint for auto-completing Assignee discloses the members of private groups.	4.3	More Details
CVE-2017-20016	A vulnerability has been found in WEKA INTEREST Security Scanner up to 1.8 and classified as problematic. This vulnerability affects unknown code of the component Portscan. The manipulation with an unknown input leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	4.3	More Details
CVE-2022-0738	An issue has been discovered in GitLab affecting all versions starting from 14.6 before 14.6.5, all versions starting from 14.7 before 14.7.4, all versions starting from 14.8 before 14.8.2. GitLab was leaking user passwords when adding mirrors with SSH credentials under specific conditions.	4.2	More Details
CVE-2022-25611	Authenticated Stored Cross-Site Scripting (XSS) in Simple Event Planner plugin <= 1.5.4 allows attackers with contributor or higher user roles to inject the malicious script by using vulnerable parameter &custom[add_seg][].	4.1	More Details
CVE-2022-25612	Multiple Authenticated Persistent Cross-Site Scripting (XSS) vulnerabilities in Simple Event Planner WordPress plugin <= 1.5.4 allows user with author or higher user rights inject the malicious code via vulnerable parameters: &custom[event_organiser], &custom[organiser_email], &custom[organiser_contact].	4.1	More Details
CVE-2022-27820	OWASP Zed Attack Proxy (ZAP) through w2022-03-21 does not verify the TLS certificate chain of an HTTPS server.	4.0	More Details
CVE-2003-5002	A vulnerability was found in ISS BlackICE PC Protection. It has been declared as problematic. Affected by this vulnerability is the component Update Handler which allows cleartext transmission of data. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24784	Statamic is a Laravel and Git powered CMS. Before versions 3.2.39 and 3.3.2, it is possible to confirm a single character of a user's password hash using a specially crafted regular expression filter in the users endpoint of the REST API. Multiple such requests can eventually uncover the entire hash. The hash is not present in the response, however the presence or absence of a result confirms if the character is in the right position. The API has throttling enabled by default, making this a time intensive task. Both the REST API and the users endpoint need to be enabled, as they are disabled by default. The issue has been fixed in versions 3.2.39 and above, and 3.3.2 and above.	3.7	More Details
CVE-2022-22935	An issue was discovered in SaltStack Salt in versions before 3002.8, 3003.4, 3004.1. A minion authentication denial of service can cause a MiTM attacker to force a minion process to stop by impersonating a master.	3.7	More Details
CVE-2022-1085	A vulnerability was found in CLTPHP up to 6.0. It has been declared as problematic. Affected by this vulnerability is the POST Parameter Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-1086	A vulnerability was found in DolphinPHP up to 1.5.0 and classified as problematic. Affected by this issue is the User Management Page. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-1087	A vulnerability, which was classified as problematic, has been found in htmly 5.3 whis affects the component Edit Profile Module. The manipulation of the field Title with script tags leads to persistent cross site scripting. The attack may be initiated remotely and requires an authentication. A simple POC has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-0861	A XML Extended entity vulnerability in McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote administrator attacker to upload a malicious XML file through the extension import functionality. The impact is limited to some access to confidential information and some ability to alter data.	3.5	More Details
CVE-2022-1075	A vulnerability was found in College Website Management System 1.0 and classified as problematic. Affected by this issue is the file /cwms/classes/Master.php?f=save_contact of the component Contact Handler. The manipulation leads to persistent cross site scripting. The attack may be launched remotely and requires authentication.	3.5	More Details
CVE-2022-0488	An issue has been discovered in GitLab CE/EE affecting all versions starting with version 8.10. It was possible to trigger a timeout on a page with markdown by using a specific amount of block-quotes.	3.5	More Details
CVE-2022-25610	Unauthenticated Stored Cross-Site Scripting (XSS) in Simple Ajax Chat <= 20220115 allows an attacker to store the malicious code. However, the attack requires specific conditions, making it hard to exploit.	3.4	More Details
CVE-2018-25030	A vulnerability classified as problematic has been found in Mirmay Secure Private Browser and File Manager up to 2.5. Affected is the Auto Lock. A race condition leads to a local authentication bypass. The exploit has been disclosed to the public and may be used.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0343	A local attacker, as a different local user, may be able to send a HTTP request to 127.0.0.1:10000 after the user (typically a developer) manually invoked the ./tools/run-dev-server script. It is recommended to upgrade to any version beyond 24.2	3.3	More Details
CVE-2022-0862	A lack of password change protection vulnerability in a depreciated API of McAfee Enterprise ePolicy Orchestrator (ePO) prior to 5.10 Update 13 allows a remote attacker to change the password of a compromised session without knowing the existing user's password. This functionality was removed from the User Interface in ePO 10 and the API has now been disabled. Other protection is in place to reduce the likelihood of this being successful through sending a link to a logged in user.	3.1	More Details
CVE-2022-0344	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 14.5.4, all versions starting from 10.1 before 14.6.4, all versions starting from 10.2 before 14.7.1. Private project paths can be disclosed to unauthorized users via system notes when an Issue is closed via a Merge Request and later moved to a public project	3.1	More Details
CVE-2022-0249	A vulnerability was discovered in GitLab starting with version 12. GitLab was vulnerable to a blind SSRF attack since requests to shared address space were not blocked.	3.1	More Details
CVE-2017-20011	A vulnerability was found in WEKA INTEREST Security Scanner 1.8. It has been rated as problematic. This issue affects some unknown processing of the component HTTP Handler. The manipulation with an unknown input leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	2.8	More Details
CVE-2017-20013	A vulnerability classified as problematic was found in WEKA INTEREST Security Scanner up to 1.8. Affected by this vulnerability is the Stresstest Configuration Handler. A manipulation leads to a local denial of service. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	2.8	More Details
CVE-2017-20015	A vulnerability, which was classified as problematic, was found in WEKA INTEREST Security Scanner up to 1.8. This affects an unknown part of the component LAN Viewer. The manipulation with an unknown input leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	2.8	More Details
CVE-2017-20014	A vulnerability, which was classified as problematic, has been found in WEKA INTEREST Security Scanner up to 1.8. Affected by this issue is some unknown functionality of the component Webspider. The manipulation with an unknown input leads to denial of service. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	2.8	More Details
CVE-2017-20012	A vulnerability classified as problematic has been found in WEKA INTEREST Security Scanner up to 1.8. Affected is Stresstest Scheme Handler which leads to a denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	2.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27456	Philips Gemini PET/CT family software stores sensitive information in a removable media device that does not have built-in access control.	2.4	More Details
CVE-2021-43085	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2022-0886	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-27666. Reason: This candidate is a reservation duplicate of CVE-2022-27666. Notes: All CVE users should reference CVE-2022-27666 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-1072	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-26254. Reason: This candidate is a reservation duplicate of CVE-2022-26254. Notes: All CVE users should reference CVE-2022-26254 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-26620	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2022-26200	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-44103	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-42192. Reason: This candidate is a duplicate of CVE-2021-42192. Notes: All CVE users should reference CVE-2021-42192 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details