SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 16 March 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-24760	Parse Server is an open source http web server backend. In versions prior to 4.10.7 there is a Remote Code Execution (RCE) vulnerability in Parse Server. This vulnerability affects Parse Server in the default configuration with MongoDB. The main weakness that leads to RCE is the Prototype Pollution vulnerable code in the file `DatabaseController.js`, so it is likely to affect Postgres and any other database backend as well. This vulnerability has been confirmed on Linux (Ubuntu) and Windows. Users are advised to upgrade as soon as possible. The only known workaround is to manually patch your installation with code referenced at the source GHSA-p6h4-93qp-jhcm.	10.0	More Details
CVE-2021-44620	A Command Injection vulnerability exits in TOTOLINK A3100R <=V4.1.2cu.5050_B20200504 in adm/ntm.asp via the hosTime parameters.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24752	SyliusGridBundle is a package of generic data grids for Symfony applications. Prior to versions 1.10.1 and 1.11-rc2, values added at the end of query sorting were passed directly to the database. The maintainers do not know if this could lead to direct SQL injections but took steps to remediate the vulnerability. The issue is fixed in versions 1.10.1 and 1.11-rc2. As a workaround, overwrite the`Sylius\Component\Grid\Sorting\Sorter.php` class and register it in the container. More information about this workaround is available in the GitHub Security Advisory.	9.8	More Details
CVE-2022-26206	Totolink A830R V5.9c.4729_B20191112, A3100R V4.1.2cu.5050_B20200504, A950RG V4.1.2cu.5161_B20200903, A800R V4.1.2cu.5137_B20200730, A3000RU V5.9c.5185_B20201128, and A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability in the function setLanguageCfg, via the langType parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-25498	CuppaCMS v1.0 was discovered to contain a remote code execution (RCE) vulnerability via the saveConfigData function in /classes/ajax/Functions.php.	9.8	More Details
CVE-2022-25495	The component /jquery_file_upload/server/php/index.php of CuppaCMS v1.0 allows attackers to upload arbitrary files and execute arbitrary code via a crafted PHP file.	9.8	More Details
CVE-2022-25494	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via staff_login.php.	9.8	More Details
CVE-2022-25492	HMS v1.0 was discovered to contain a SQL injection vulnerability via the medicineid parameter in ajaxmedicine.php.	9.8	More Details
CVE-2022-25490	HMS v1.0 was discovered to contain a SQL injection vulnerability via the editid parameter in department.php.	9.8	More Details
CVE-2022-25488	Atom CMS v2.0 was discovered to contain a SQL injection vulnerability via the id parameter in /admin/ajax/avatar.php.	9.8	More Details
CVE-2022-25487	Atom CMS v2.0 was discovered to contain a remote code execution (RCE) vulnerability via /admin/uploads.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0658	The CommonsBooking WordPress plugin before 2.6.8 does not sanitise and escape the location parameter of the calendar_data AJAX action (available to unauthenticated users) before it is used in dynamically constructed SQL queries, leading to an unauthenticated SQL injection	9.8	More Details
CVE-2022-26208	Totolink A830R V5.9c.4729_B20191112, A3100R V4.1.2cu.5050_B20200504, A950RG V4.1.2cu.5161_B20200903, A800R V4.1.2cu.5137_B20200730, A3000RU V5.9c.5185_B20201128, and A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability in the function setWebWlanIdx, via the webWlanIdx parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-0254	The WordPress Zero Spam WordPress plugin before 5.2.11 does not properly sanitise and escape the order and orderby parameters before using them in a SQL statement in the admin dashboard, leading to a SQL injection	9.8	More Details
CVE-2022-0169	The Photo Gallery by 10Web WordPress plugin before 1.6.0 does not validate and escape the bwg_tag_id_bwg_thumbnails_0 parameter before using it in a SQL statement via the bwg_frontend_data AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL injection	9.8	More Details
CVE-2021-25007	The MOLIE WordPress plugin through 0.5 does not validate and escape a post parameter before using in a SQL statement, leading to an SQL Injection	9.8	More Details
CVE-2021-25003	The WPCargo Track & Trace WordPress plugin before 6.9.0 contains a file which could allow unauthenticated attackers to write a PHP file anywhere on the web server, leading to RCE	9.8	More Details
CVE-2022-23943	Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.	9.8	More Details
CVE-2022-22720	Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling	9.8	More Details
CVE-2021-45887	An issue was discovered in PONTON X/P Messenger before 3.11.2. Due to path traversal in private/SchemaSetUpload.do for uploaded ZIP files, an executable script can be uploaded by web application administrators, giving the attacker remote code execution on the underlying server via an imgs/*.jsp URI.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25621	UUNIVERGE WA 1020 Ver8.2.11 and prior, UNIVERGE WA 1510 Ver8.2.11 and prior, UNIVERGE WA 1511 Ver8.2.11 and prior, UNIVERGE WA 1512 Ver8.2.11 and prior, UNIVERGE WA 2020 Ver8.2.11 and prior, UNIVERGE WA 2021 Ver8.2.11 and prior, UNIVERGE WA 2610-AP Ver8.2.11 and prior, UNIVERGE WA 2611-AP Ver8.2.11 and prior, UNIVERGE WA 2611E-AP Ver8.2.11 and prior, UNIVERGE WA WA2612-AP Ver8.2.11 and prior allows a remote attacker to execute arbitrary OS commands.	9.8	More Details
CVE-2022-26207	Totolink A830R V5.9c.4729_B20191112, A3100R V4.1.2cu.5050_B20200504, A950RG V4.1.2cu.5161_B20200903, A800R V4.1.2cu.5137_B20200730, A3000RU V5.9c.5185_B20201128, and A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability in the function setDiagnosisCfg, via the ipDoamin parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-26209	Totolink A830R V5.9c.4729_B20191112, A3100R V4.1.2cu.5050_B20200504, A950RG V4.1.2cu.5161_B20200903, A800R V4.1.2cu.5137_B20200730, A3000RU V5.9c.5185_B20201128, and A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability in the function setUploadSetting, via the FileName parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2021-44618	A Server-side Template Injection (SSTI) vulnerability exists in Nystudio107 Seomatic 3.4.12 in src/helpers/UrlHelper.php via the host header.	9.8	More Details
CVE-2022-26210	Totolink A830R V5.9c.4729_B20191112, A3100R V4.1.2cu.5050_B20200504, A950RG V4.1.2cu.5161_B20200903, A800R V4.1.2cu.5137_B20200730, A3000RU V5.9c.5185_B20201128, and A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability in the function setUpgradeFW, via the FileName parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-27004	Totolink routers s X5000R V9.1.0u.6118_B20201102 and A7000R V9.1.0u.6115_B20201022 were discovered to contain a command injection vulnerability in the Tunnel 6in4 function via the remote6in4 parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27003	Totolink routers s X5000R V9.1.0u.6118_B20201102 and A7000R V9.1.0u.6115_B20201022 were discovered to contain a command injection vulnerability in the Tunnel 6rd function via the relay6rd parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-27002	Arris TR3300 v1.0.13 were discovered to contain a command injection vulnerability in the ddns function via the ddns_name, ddns_pwd, h_ddns、ddns_host parameters. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-27001	Arris TR3300 v1.0.13 were discovered to contain a command injection vulnerability in the dhcp function via the hostname parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-27000	Arris TR3300 v1.0.13 was discovered to contain a command injection vulnerability in the time and time zone function via the h_primary_ntp_server, h_backup_ntp_server, and h_time_zone parameters. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-26999	Arris TR3300 v1.0.13 was discovered to contain a command injection vulnerability in the static ip settings function via the wan_ip_stat, wan_mask_stat, wan_gw_stat, and wan_dns1_stat parameters. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-26998	Arris TR3300 v1.0.13 was discovered to contain a command injection vulnerability in the wps setting function via the wps_enrolee_pin parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-26997	Arris TR3300 v1.0.13 was discovered to contain a command injection vulnerability in the upnp function via the upnp_ttl parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-26996	Arris TR3300 v1.0.13 was discovered to contain a command injection vulnerability in the pppoe function via the pppoe_username, pppoe_passwd, and pppoe_servicename parameters. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26995	Arris TR3300 v1.0.13 was discovered to contain a command injection vulnerability in the pptp (wan_pptp.html) function via the pptp_fix_ip, pptp_fix_mask, pptp_fix_gw, and wan_dns1_stat parameters. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-26994	Arris routers SBR-AC1900P 1.0.7-B05, SBR-AC3200P 1.0.7-B05 and SBR-AC1200P 1.0.5-B05 were discovered to contain a command injection vulnerability in the pptp function via the pptpUserName and pptpPassword parameters. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-26993	Arris routers SBR-AC1900P 1.0.7-B05, SBR-AC3200P 1.0.7-B05 and SBR-AC1200P 1.0.5-B05 were discovered to contain a command injection vulnerability in the pppoe function via the pppoeUserName, pppoePassword, and pppoe_Service parameters. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-26992	Arris routers SBR-AC1900P 1.0.7-B05, SBR-AC3200P 1.0.7-B05 and SBR-AC1200P 1.0.5-B05 were discovered to contain a command injection vulnerability in the ddns function via the DdnsUserName, DdnsHostName, and DdnsPassword parameters. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-26991	Arris routers SBR-AC1900P 1.0.7-B05, SBR-AC3200P 1.0.7-B05 and SBR-AC1200P 1.0.5-B05 were discovered to contain a command injection vulnerability in the ntp function via the TimeZone parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-26990	Arris routers SBR-AC1900P 1.0.7-B05, SBR-AC3200P 1.0.7-B05 and SBR-AC1200P 1.0.5-B05 were discovered to contain a command injection vulnerability in the firewall-local log function via the EmailAddress, SmtpServerName, SmtpUsername, and SmtpPassword parameters. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-26214	Totolink A830R V5.9c.4729_B20191112, A3100R V4.1.2cu.5050_B20200504, A950RG V4.1.2cu.5161_B20200903, A800R V4.1.2cu.5137_B20200730, A3000RU V5.9c.5185_B20201128, and A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability in the function NTPSyncWithHost. This vulnerability allows attackers to execute arbitrary commands via the host_time parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26213	Totolink X5000R_Firmware v9.1.0u.6118_B20201102 was discovered to contain a command injection vulnerability in the function setNtpCfg, via the tz parameters. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-26212	Totolink A830R V5.9c.4729_B20191112, A3100R V4.1.2cu.5050_B20200504, A950RG V4.1.2cu.5161_B20200903, A800R V4.1.2cu.5137_B20200730, A3000RU V5.9c.5185_B20201128, and A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability in the function setDeviceName, via the deviceMac and deviceName parameters. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-26211	Totolink A830R V5.9c.4729_B20191112, A3100R V4.1.2cu.5050_B20200504, A950RG V4.1.2cu.5161_B20200903, A800R V4.1.2cu.5137_B20200730, A3000RU V5.9c.5185_B20201128, and A810R V4.1.2cu.5182_B20201026 were discovered to contain a command injection vulnerability in the function CloudACMunualUpdate, via the deviceMac and deviceName parameters. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-23730	The public API error causes for the attacker to be able to bypass API access control.	9.8	More Details
CVE-2022-27005	Totolink routers s X5000R V9.1.0u.6118_B20201102 and A7000R V9.1.0u.6115_B20201022 were discovered to contain a command injection vulnerability in the setWanCfg function via the hostName parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	9.8	More Details
CVE-2022-24603	Luocms v2.0 is affected by SQL Injection in /admin/news/sort_mod.php.	9.8	More Details
CVE-2021-44629	A Buffer Overflow vulnerabilitiy exists in TP-LINK WR-886N 20190826 2.3.8 in the /cloud_config/router_post/register feature, which allows malicious users to execute arbitrary code on the system via a crafted post request.	9.8	More Details
CVE-2022-24600	Luocms v2.0 is affected by SQL Injection through /admin/login.php. An attacker can log in to the background through SQL injection statements.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24193	CasaOS before v0.2.7 was discovered to contain a command injection vulnerability.	9.8	More Details
CVE-2022-22814	The System Diagnosis service of MyASUS before 3.1.2.0 allows privilege escalation.	9.8	More Details
CVE-2021-4045	TP-Link Tapo C200 IP camera, on its 1.1.15 firmware version and below, is affected by an unauthenticated RCE vulnerability, present in the uhttpd binary running by default as root. The exploitation of this vulnerability allows an attacker to take full control of the camera.	9.8	More Details
CVE-2021-44632	A Buffer Overflow vulnerability exists in TP-LINK WR-886N 20190826 2.3.8 in the /cloud_config/router_post/upgrade_info feature, which allows malicious users to execute arbitrary code on the system via a crafted post request.	9.8	More Details
CVE-2021-44631	A Buffer Overflow vulnerability exists in TP-LINK WR-886N 20190826 2.3.8 in the /cloud_config/router_post/reset_cloud_pwd feature, which allows malicous users to execute arbitrary code on the system via a crafted post request.	9.8	More Details
CVE-2021-44630	A Buffer Overflow vulnerability exists in TP-LINK WR-886N 20190826 2.3.8 in the /cloud_config/router_post/modify_account_pwd feature, which allows malicious users to execute arbitrary code on the system via a crafted post request.	9.8	More Details
CVE-2021-44628	A Buffer Overflow vulnerabiltiy exists in TP-LINK WR-886N 20190826 2.3.8 in thee /cloud_config/router_post/login feature, which allows malicious users to execute arbitrary code on the system via a crafted post request.	9.8	More Details
CVE-2022-24604	Luocms v2.0 is affected by SQL Injection in /admin/link/link_mod.php.	9.8	More Details
CVE-2021-44627	A Buffer Overflow vulnerability exists in TP-LINK WR-886N 20190826 2.3.8 in the /cloud_config/router_post/get_reset_pwd_veirfy_code feature, which allows malicious users to execute arbitrary code on the system via a crafted post request.	9.8	More Details
CVE-2021-44626	A Buffer Overflow vulnerability exists in TP-LINK WR-886N 20190826 2.3.8 in the /cloud_config/router_post/get_reg_verify_code feature, which allows malicious users to execute arbitrary code on the system via a crafted post request.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44625	A Buffer Overflow vulnerability exists in TP-LINK WR-886N 20190826 2.3.8 in /cloud_config/cloud_device/info interface, which allows a malicious user to executee arbitrary code on the system via a crafted post request.	9.8	More Details
CVE-2021-44623	A Buffer Overflow vulnerability exists in TP-LINK WR-886N 20190826 2.3.8 via the /cloud_config/router_post/check_reset_pwd_verify_code interface.	9.8	More Details
CVE-2021-44622	A Buffer Overflow vulnerability exists in TP-LINK WR-886N 20190826 2.3.8 in the /cloud_config/router_post/check_reg_verify_code function which could let a remove malicious user execute arbitrary code via a crafted post request.	9.8	More Details
CVE-2021-42854	It was discovered that the SteelCentral AppInternals Dynamic Sampling Agent's (DSA) PluginServlet has directory traversal vulnerabilities at the "/api/appInternals/1.0/plugin/pmx" API. The affected endpoint does not have any input validation of the user's input that allows a malicious payload to be injected.	9.8	More Details
CVE-2021-40050	There is an out-of-bounds read vulnerability in the IFAA module. Successful exploitation of this vulnerability may cause stack overflow.	9.8	More Details
CVE-2022-24602	Luocms v2.0 is affected by SQL Injection in /admin/news/news_mod.php.	9.8	More Details
CVE-2021-42786	It was discovered that the SteelCentral AppInternals Dynamic Sampling Agent (DSA) has Remote Code Execution vulnerabilities in multiple instances of the API requests. The affected endpoints do not have any input validation of the user's input that allowed a malicious payload to be injected.	9.8	More Details
CVE-2022-26100	SAPCAR - version 7.22, does not contain sufficient input validation on the SAPCAR archive. As a result, the SAPCAR process may crash, and the attacker may obtain privileged access to the system.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22805	A CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability exists that could cause remote code execution when an improperly handled TLS packet is reassembled. Affected Product: SmartConnect Family: SMT Series (SMT Series ID=1015: UPS 04.5 and prior), SMC Series (SMC Series ID=1018: UPS 04.2 and prior), SMTL Series (SMTL Series ID=1026: UPS 02.9 and prior), SCL Series (SCL Series ID=1029: UPS 02.5 and prior / SCL Series ID=1030: UPS 02.5 and prior / SCL Series ID=1036: UPS 02.5 and prior / SCL Series ID=1037: UPS 03.1 and prior), SMX Series (SMX Series ID=1031: UPS 03.1 and prior)	9.8	More Details
CVE-2022-21194	The following Yokogawa Electric products do not change the passwords of the internal Windows accounts from the initial configuration: CENTUM VP versions from R5.01.00 to R5.04.20 and versions from R6.01.00 to R6.08.0, Exaopc versions from R3.72.00 to R3.79.00.	9.8	More Details
CVE-2022-26520	In pgjdbc before 42.3.3, an attacker (who controls the jdbc URL or properties) can call java.util.logging.FileHandler to write to arbitrary files through the loggerFile and loggerLevel connection properties. An example situation is that an attacker could create an executable JSP file under a Tomcat web root. NOTE: the vendor's position is that there is no pgjdbc vulnerability; instead, it is a vulnerability for any application to use the pgjdbc driver with untrusted connection properties	9.8	More Details
CVE-2022-26143	The TP-240 (aka tp240dvr) component in Mitel MiCollab before 9.4 SP1 FP1 and MiVoice Business Express through 8.1 allows remote attackers to obtain sensitive information and cause a denial of service (performance degradation and excessive outbound traffic). This was exploited in the wild in February and March 2022 for the TP240PhoneHome DDoS attack.	9.8	More Details
CVE-2022-22806	A CWE-294: Authentication Bypass by Capture-replay vulnerability exists that could cause an unauthenticated connection to the UPS when a malformed connection is sent. Affected Product: SmartConnect Family: SMT Series (SMT Series ID=1015: UPS 04.5 and prior), SMC Series (SMC Series ID=1018: UPS 04.2 and prior), SMTL Series (SMTL Series ID=1026: UPS 02.9 and prior), SCL Series (SCL Series ID=1029: UPS 02.5 and prior / SCL Series ID=1030: UPS 02.5 and prior / SCL Series ID=1036: UPS 02.5 and prior / SCL Series ID=1037: UPS 03.1 and prior), SMX Series (SMX Series ID=1031: UPS 03.1 and prior)	9.8	More Details
CVE-2022-0895	Static Code Injection in GitHub repository microweber/microweber prior to 1.3.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24605	Luocms v2.0 is affected by SQL Injection in /admin/link/link_ok.php.	9.8	More Details
CVE-2022-24995	Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the time parameter.	9.8	More Details
CVE-2022-24652	sentcms 4.0.x allows remote attackers to cause arbitrary file uploads through an unauthorized file upload interface, resulting in php code execution in /admin/upload/upload.	9.8	More Details
CVE-2022-24651	sentcms 4.0.x allows remote attackers to cause arbitrary file uploads through an unauthorized file upload interface, resulting in PHP code execution through /user/upload/upload.	9.8	More Details
CVE-2022-24609	Luocms v2.0 is affected by an incorrect access control vulnerability. Through /admin/templates/template_manage.php, an attacker can write an arbitrary shell file.	9.8	More Details
CVE-2020-14115	A command injection vulnerability exists in the Xiaomi Router AX3600. The vulnerability is caused by a lack of inspection for incoming data detection. Attackers can exploit this vulnerability to execute code.	9.8	More Details
CVE-2022-24607	Luocms v2.0 is affected by SQL Injection in /admin/news/news_ok.php.	9.8	More Details
CVE-2022-24606	Luocms v2.0 is affected by SQL Injection in /admin/news/sort_ok.php.	9.8	More Details
CVE-2022-23402	The following Yokogawa Electric products hard-code the password for CAMS server applications: CENTUM VP versions from R5.01.00 to R5.04.20 and versions from R6.01.00 to R6.08.00, Exaopc versions from R3.72.00 to R3.79.00	9.8	More Details
CVE-2021-42787	It was discovered that the SteelCentral AppInternals Dynamic Sampling Agent's (DSA) AgentConfigurationServlet has directory traversal vulnerabilities at the "/api/appInternals/1.0/agent/configuration" API. The affected endpoint does not have any input validation of the user's input that allows a malicious payload to be injected.	9.4	More Details
CVE-2022-26131	Power Line Communications PLC4TRUCKS J2497 trailer receivers are susceptible to remote RF induced signals.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40053	There is a permission control vulnerability in the Nearby module.Successful exploitation of this vulnerability will affect availability and integrity.	9.1	More Details
CVE-2021-33293	Panorama Tools libpano13 v2.9.20 was discovered to contain an out-of-bounds read in the function panoParserFindOLine() in parser.c.	9.1	More Details
CVE-2022-0860	Improper Authorization in GitHub repository cobbler/cobbler prior to 3.3.2.	9.1	More Details
CVE-2022-23383	YzmCMS v6.3 is affected by broken access control. Without login, unauthorized access to the user's personal home page can be realized. It is necessary to judge the user's login status before accessing the personal home page, but the vulnerability can access other users' home pages through the non login status because real authentication is not carried out.	9.1	More Details
CVE-2021-42853	It was discovered that the SteelCentral AppInternals Dynamic Sampling Agent's (DSA) AgentDiagnosticServlet has directory traversal vulnerability at the "/api/appInternals/1.0/agent/diagnostic/logs" API. The affected endpoint does not have any input validation of the user's input that allows a malicious payload to be injected.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0715	A CWE-287: Improper Authentication vulnerability exists that could cause an attacker to arbitrarily change the behavior of the UPS when a key is leaked and used to upload malicious firmware. Affected Product: APC Smart-UPS Family: SMT Series (SMT Series ID=18: UPS 09.8 and prior / SMT Series ID=1040: UPS 01.2 and prior / SMT Series ID=1031: UPS 03.1 and prior), SMC Series (SMC Series ID=1005: UPS 14.1 and prior / SMC Series ID=1007: UPS 11.0 and prior / SMC Series ID=1041: UPS 01.1 and prior), SCL Series (SCL Series ID=1030: UPS 02.5 and prior / SCL Series ID=1036: UPS 02.5 and prior), SMX Series (SMX Series ID=20: UPS 10.2 and prior / SMX Series ID=23: UPS 07.0 and prior), SRT Series (SRT Series ID=1010/1019/1025: UPS 08.3 and prior / SRT Series ID=1024: UPS 01.0 and prior / SRT Series ID=1020: UPS 10.4 and prior / SRT Series ID=1021: UPS 12.2 and prior / SRT Series ID=1001/1013: UPS 05.1 and prior / SRT Series ID=1002/1014: UPSa05.2 and prior), APC SmartConnect Family: SMT Series (SMT Series ID=1015: UPS 04.5 and prior), SMC Series (SMC Series ID=1018: UPS 04.2 and prior), SMTL Series (SMTL Series ID=1026: UPS 02.9 and prior), SCL Series (SCL Series ID=1029: UPS 02.5 and prior / SCL Series ID=1030: UPS 02.5 and prior / SCL Series ID=1036: UPS 02.5 and prior / SCL Series ID=1037: UPS 03.1 and prior), SMX Series (SMX Series ID=1031: UPS 03.1 and prior)	9.1	More Details
CVE-2022-26320	The Rambus SafeZone Basic Crypto Module before 10.4.0, as used in certain Fujifilm (formerly Fuji Xerox) devices before 2022-03-01, Canon imagePROGRAF and imageRUNNER devices through 2022-03-14, and potentially many other devices, generates RSA keys that can be broken with Fermat's factorization method. This allows efficient calculation of private RSA keys from the public key of a TLS certificate.	9.1	More Details
CVE-2022-24387	With administrator or admin privileges the application can be tricked into overwriting files in app_data/Config folder, e.g. the systemsettings.xml file. THis is possible in SmarterTrack v100.0.8019.14010	9.1	More Details
CVE-2022-22721	If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.	9.1	More Details
CVE-2022-0871	Missing Authorization in GitHub repository gogs/gogs prior to 0.12.5.	9.1	More Details
CVE-2022-0482	Exposure of Private Personal Information to an Unauthorized Actor in GitHub repository alextselegidis/easyappointments prior to 1.4.3.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-26846	SPIP before 3.2.14 and 4.x before 4.0.5 allows remote authenticated editors to execute arbitrary code.	8.8	More Details
CVE-2022-24508	Win32 File Enumeration Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-43305	Heap buffer overflow in Clickhouse's LZ4 compression codec when parsing a malicious query. There is no verification that the copy operations in the LZ4::decompressImpl loop and especially the arbitrary copy operation wildCopy<copy_amount>(op, ip, copy_end), don't exceed the destination buffer's limits. This issue is very similar to CVE-2021-43304, but the vulnerable copy operation is in a different wildCopy call.	8.8	More Details
CVE-2022-0204	A heap overflow vulnerability was found in bluez in versions prior to 5.63. An attacker with local network access could pass specially crafted files causing an application to halt or crash, leading to a denial of service.	8.8	More Details
CVE-2022-23294	Windows Event Tracing Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-24644	ZZ Inc. KeyMouse Windows 3.08 and prior is affected by a remote code execution vulnerability during an unauthenticated update. To exploit this vulnerability, a user must trigger an update of an affected installation of KeyMouse.	8.8	More Details
CVE-2021-43304	Heap buffer overflow in Clickhouse's LZ4 compression codec when parsing a malicious query. There is no verification that the copy operations in the LZ4::decompressImpl loop and especially the arbitrary copy operation wildCopy<copy_amount>(op, ip, copy_end), don't exceed the destination buffer's limits.	8.8	More Details
CVE-2021-45886	An issue was discovered in PONTON X/P Messenger before 3.11.2. Anti-CSRF tokens are globally valid, making the web application vulnerable to a weakened version of CSRF, where an arbitrary token of a low-privileged user (such as operator) can be used to confirm actions of higher-privileged ones (such as xpadmin).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22729	CAMS for HIS Server contained in the following Yokogawa Electric products improperly authenticate the receiving packets. The authentication may be bypassed via some crafted packets: CENTUM CS 3000 versions from R3.08.10 to R3.09.00, CENTUM VP versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, and from R6.01.00 to R6.08.00, and Exaopc versions from R3.72.00 to R3.79.00.	8.8	More Details
CVE-2022-24384	Cross-site Scripting (XSS) vulnerability in SmarterTools SmarterTrack This issue affects: SmarterTools SmarterTrack 100.0.8019.14010.	8.8	More Details
CVE-2022-24386	Stored XSS in SmarterTools SmarterTrack This issue affects: SmarterTools SmarterTrack 100.0.8019.14010.	8.8	More Details
CVE-2022-23285	Remote Desktop Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-21808	Path traversal vulnerability exists in CAMS for HIS Server contained in the following Yokogawa Electric products: CENTUM CS 3000 versions from R3.08.10 to R3.09.00, CENTUM VP versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, and from R6.01.00 to R6.08.00, Exaopc versions from R3.72.00 to R3.79.00.	8.8	More Details
CVE-2021-24959	The WP Email Users WordPress plugin through 1.7.6 does not escape the data_raw parameter in the weu_selected_users_1 AJAX action, available to any authenticated users, allowing them to perform SQL injection attacks.	8.8	More Details
CVE-2021-43970	An arbitrary file upload vulnerability exists in albumimages.jsp in Quicklert for Digium 10.0.0 (1043) via a .mp3;.jsp filename for a file that begins with audio data bytes. It allows an authenticated (low privileged) attacker to execute remote code on the target server within the context of application's permissions (SYSTEM).	8.8	More Details
CVE-2022-0478	The Event Manager and Tickets Selling for WooCommerce WordPress plugin before 3.5.8 does not validate and escape the post_author_gutenberg parameter before using it in a SQL statement when creating/editing events, which could allow users with a role as low as contributor to perform SQL Injection attacks	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22735	The Simple Quotation WordPress plugin through 1.3.2 does not have authorisation (and CSRF) checks in various of its AJAX actions and is lacking escaping of user data when using it in SQL statements, allowing any authenticated users, such as subscriber to perform SQL injection attacks	8.8	More Details
CVE-2022-25510	FreeTAKServer 1.9.8 contains a hardcoded Flask secret key which allows attackers to create crafted cookies to bypass authentication or escalate privileges.	8.8	More Details
CVE-2022-22346	IBM Spectrum Protect Operations Center 8.1.0.000 through 8.1.13.xxx is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 220048.	8.8	More Details
CVE-2022-24750	UltraVNC is a free and open source remote pc access software. A vulnerability has been found in versions prior to 1.3.8.0 in which the DSM plugin module, which allows a local authenticated user to achieve local privilege escalation (LPE) on a vulnerable system. The vulnerability has been fixed to allow loading of plugins from the installed directory. Affected users should upgrade their UltraVNC to 1.3.8.1. Users unable to upgrade should not install and run UltraVNC server as a service. It is advisable to create a scheduled task on a low privilege account to launch WinVNC.exe instead. There are no known workarounds if winvnc needs to be started as a service.	8.8	More Details
CVE-2021-44673	A Remote Code Execution (RCE) vulnerability exists in Croogo 3.0.2via admin/file-manager/attachments, which lets a malcoius user upload a web shell script.	8.8	More Details
CVE-2021-45010	A path traversal vulnerability in the file upload functionality in tinyfilemanager.php in Tiny File Manager before 2.4.7 allows remote attackers (with valid user accounts) to upload malicious PHP files to the webroot, leading to code execution.	8.8	More Details
CVE-2021-39022	IBM Guardium Data Encryption (GDE) 4.0.0.0 and 5.0.0.0 saves user-provided information into a Comma-Separated Value (CSV) file, but it does not neutralize or incorrectly neutralizes special elements that could be interpreted as a command when the file is opened by spreadsheet software. IBM X-Force ID: 213858.	8.8	More Details
CVE-2022-21990	Remote Desktop Client Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22985	The absence of filters when loading some sections in the web application of the vulnerable device allows attackers to inject malicious code that will be interpreted when a legitimate user accesses the specific web section where the information is displayed. Injection can be done on specific parameters. The injected code is executed when a legitimate user attempts to review history.	8.8	More Details
CVE-2022-27204	A cross-site request forgery vulnerability in Jenkins Extended Choice Parameter Plugin 346.vd87693c5a_86c and earlier allows attackers to connect to an attacker-specified URL.	8.8	More Details
CVE-2022-22771	The Server component of TIBCO Software Inc.'s TIBCO JasperReports Library, TIBCO JasperReports Library for ActiveMatrix BPM, TIBCO JasperReports Server, TIBCO JasperReports Server for AWS Marketplace, TIBCO JasperReports Server for ActiveMatrix BPM, and TIBCO JasperReports Server for Microsoft Azure contains a directory-traversal vulnerability that may theoretically allow web server users to access contents of the host system. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Library: version 7.9.0, TIBCO JasperReports Library for ActiveMatrix BPM: version 7.9.0, TIBCO JasperReports Server: versions 7.9.0 and 7.9.1, TIBCO JasperReports Server for AWS Marketplace: versions 7.9.0 and 7.9.1, TIBCO JasperReports Server for ActiveMatrix BPM: versions 7.9.0 and 7.9.1, and TIBCO JasperReports Server for Microsoft Azure: version 7.9.1.	8.8	More Details
CVE-2022-23940	SuiteCRM through 7.12.1 and 8.x through 8.0.1 allows Remote Code Execution. Authenticated users with access to the Scheduled Reports module can achieve this by leveraging PHP deserialization in the email_recipients property. By using a crafted request, they can create a malicious report, containing a PHP-deserialization payload in the email_recipients field. Once someone accesses this report, the backend will deserialize the content of the email_recipients field and the payload gets executed. Project dependencies include a number of interesting PHP deserialization gadgets (e.g., Monolog/RCE1 from phpggc) that can be used for Code Execution.	8.8	More Details
CVE-2022-23277	Microsoft Exchange Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-22834	An issue was discovered in OverIT Geocall before 8.0. An authenticated user who has the Test Trasformazione XSL functionality enabled can exploit a XSLT Injection vulnerability. Attackers could exploit this issue to achieve remote code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22783	A CWE-200: Information Exposure vulnerability exists which could allow a session hijack when the door panel is communicating with the door. Affected Product: Ritto Wiser Door (All versions)	8.8	More Details
CVE-2022-0896	Improper Neutralization of Special Elements Used in a Template Engine in GitHub repository microweber/microweber prior to 1.3.	8.8	More Details
CVE-2022-24754	PJSIP is a free and open source multimedia communication library written in C language. In versions prior to and including 2.12 PJSIP there is a stack-buffer overflow vulnerability which only impacts PJSIP users who accept hashed digest credentials (credentials with data_type \`PJSIP_CRED_DATA_DIGEST\`). This issue has been patched in the master branch of the PJSIP repository and will be included with the next release. Users unable to upgrade need to check that the hashed digest data length must be equal to \`PJSIP_MD5STRLEN\` before passing to PJSIP.	8.5	More Details
CVE-2022-25219	A null byte interaction error has been discovered in the code that the telnetd_startup daemon uses to construct a pair of ephemeral passwords that allow a user to spawn a telnet service on the router, and to ensure that the telnet service persists upon reboot. By means of a crafted exchange of UDP packets, an unauthenticated attacker on the local network can leverage this null byte interaction error in such a way as to make those ephemeral passwords predictable (with 1-in-94 odds). Since the attacker must manipulate data processed by the OpenSSL function RSA_public_decrypt(), successful exploitation of this vulnerability depends on the use of an unpadded RSA cipher (CVE-2022-25218).	8.4	More Details
CVE-2022-23927	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.	8.2	More Details
CVE-2022-23931	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.	8.2	More Details
CVE-2022-23930	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23934	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.	8.2	More Details
CVE-2022-23933	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.	8.2	More Details
CVE-2022-24416	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution during SMM.	8.2	More Details
CVE-2022-24415	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution during SMM.	8.2	More Details
CVE-2022-24421	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution during SMM.	8.2	More Details
CVE-2022-23925	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.	8.2	More Details
CVE-2022-23924	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.	8.2	More Details
CVE-2022-24420	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution during SMM.	8.2	More Details
CVE-2022-24419	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by using an SMI to gain arbitrary code execution during SMM.	8.2	More Details
CVE-2022-23926	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23932	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.	8.2	More Details
CVE-2022-23929	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.	8.2	More Details
CVE-2022-23928	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products which may allow Escalation of Privilege, Arbitrary Code Execution, Unauthorized Code Execution, Denial of Service, and Information Disclosure.	8.2	More Details
CVE-2022-24433	The package simple-git before 3.3.0 are vulnerable to Command Injection via argument injection. When calling the .fetch(remote, branch, handlerFn) function, both the remote and branch parameters are passed to the git fetch subcommand. By injecting some git options it was possible to get arbitrary command execution.	8.1	More Details
CVE-2022-25218	The use of the RSA algorithm without OAEP, or any other padding scheme, in telnetd_startup, allows an unauthenticated attacker on the local area network to achieve a significant degree of control over the "plaintext" to which an arbitrary blob of ciphertext will be decrypted by OpenSSL's RSA_public_decrypt() function. This weakness allows the attacker to manipulate the various iterations of the telnetd startup state machine and eventually obtain a root shell on the device, by means of an exchange of crafted UDP packets. In all versions but K2 22.5.9.163 and K3C 32.1.15.93 a successful attack also requires the exploitation of a null-byte interaction error (CVE-2022-25219).	8.1	More Details
CVE-2021-42387	Heap out-of-bounds read in Clickhouse's LZ4 compression codec when parsing a malicious query. As part of the LZ4::decompressImpl() loop, a 16-bit unsigned user-supplied value ('offset') is read from the compressed data. The offset is later used in the length of a copy operation, without checking the upper bounds of the source of the copy operation.	8.1	More Details
CVE-2022-21187	The package libvcs before 0.11.1 are vulnerable to Command Injection via argument injection. When calling the update_repo function (when using hg), the url parameter is passed to the hg clone command. By injecting some hg options it was possible to get arbitrary command execution.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42388	Heap out-of-bounds read in Clickhouse's LZ4 compression codec when parsing a malicious query. As part of the LZ4::decompressImpl() loop, a 16-bit unsigned user-supplied value ('offset') is read from the compressed data. The offset is later used in the length of a copy operation, without checking the lower bounds of the source of the copy operation.	8.1	More Details
CVE-2022-22151	CAMS for HIS Log Server contained in the following Yokogawa Electric products fails to properly neutralize log outputs: CENTUM CS 3000 versions from R3.08.10 to R3.09.00, CENTUM VP versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, and from R6.01.00 to R6.08.00, and Exaopc versions from R3.72.00 to R3.79.00.	8.1	More Details
CVE-2022-25090	Printix Secure Cloud Print Management through 1.3.1106.0 creates a temporary temp.ini file in a directory with insecure permissions, leading to privilege escalation because of a race condition.	8.1	More Details
CVE-2022-24721	CometD is a scalable comet implementation for web messaging. In any version prior to 5.0.11, 6.0.6, and 7.0.6, internal usage of Oort and Seti channels is improperly authorized, so any remote user could subscribe and publish to those channels. By subscribing to those channels, a remote user may be able to watch cluster-internal traffic that contains other users' (possibly sensitive) data. By publishing to those channels, a remote user may be able to create/modify/delete other user's data and modify the cluster structure. A fix is available in versions 5.0.11, 6.0.6, and 7.0.6. As a workaround, install a custom `SecurityPolicy` that forbids subscription and publishing to remote, non-Oort, sessions on Oort and Seti channels.	8.1	More Details
CVE-2022-22145	CAMS for HIS Log Server contained in the following Yokogawa Electric products is vulnerable to uncontrolled resource consumption. CENTUM CS 3000 versions from R3.08.10 to R3.09.00, CENTUM VP versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, from R6.01.00 to R6.08.00, Exaopc versions from R3.72.00 to R3.79.00.	8.1	More Details
CVE-2022-24755	Bareos is open source software for backup, archiving, and recovery of data for operating systems. When Bareos Director >= 18.2 >= 18.2 but prior to 21.1.0, 20.0.6, and 19.2.12 is built and configured for PAM authentication, it will skip authorization checks completely. Expired accounts and accounts with expired passwords can still login. This problem will affect users that have PAM enabled. Currently there is no authorization (e.g. check for expired or disabled accounts), but only plain authentication (i.e. check if username and password match). Bareos Director versions 21.1.0, 20.0.6 and 19.2.12 implement the authorization check that was previously missing. The only workaround is to make sure that authentication fails if the user is not authorized.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21177	There is a path traversal vulnerability in CAMS for HIS Log Server contained in the following Yokogawa Electric products: CENTUM CS 3000 versions from R3.08.10 to R3.09.00, CENTUM VP versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, andfrom R6.01.00 to R6.08.00, Exaopc versions from R3.72.00 to R3.79.00.	8.1	More Details
CVE-2022-24469	Azure Site Recovery Elevation of Privilege Vulnerability	8.1	More Details
CVE-2021-36777	A Reliance on Untrusted Inputs in a Security Decision vulnerability in the login proxy of the openSUSE Build service allowed attackers to present users with a expected login form that then sends the clear text credentials to an attacker specified server. This issue affects: openSUSE Build service login-proxy-scripts versions prior to dc000cdfe9b9b715fb92195b1a57559362f689ef.	8.1	More Details
CVE-2022-27198	A cross-site request forgery (CSRF) vulnerability in Jenkins CloudBees AWS Credentials Plugin 189.v3551d5642995 and earlier allows attackers with Overall/Read permission to connect to an AWS service using an attacker-specified token.	8.0	More Details
CVE-2022-24915	The absence of filters when loading some sections in the web application of the vulnerable device allows attackers to inject malicious code that will be interpreted when a legitimate user accesses the web section where the information is displayed. Injection can be done on specific parameters. The injected code is executed when a legitimate user attempts to upload, copy, download, or delete an existing configuration (Administrative Services).	8.0	More Details
CVE-2022-24128	Timescale TimescaleDB 1.x and 2.x before 2.5.2 may allow privilege escalation during extension installation. The installation process uses commands such as CREATE x IF NOT EXIST that allow an unprivileged user to precreate objects. These objects will be used by the installer (which executes as Superuser), leading to privilege escalation. In order to be able to take advantage of this, an unprivileged user would need to be able to create objects in a database and then get a Superuser to install TimescaleDB into their database. (In the fixed versions, the installation aborts when it finds that an object already exists.)	8.0	More Details
CVE-2022-24931	Improper access control vulnerability in dynamic receiver in ApkInstaller prior to SMR MAR-2022 Release allows unauthorized attackers to execute arbitrary activity without a proper permission	7.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24285	Acer Care Center 4.00.30xx before 4.00.3042 contains a local privilege escalation vulnerability. The user process communicates with a service of system authority called ACCsvc through a named pipe. In this case, the Named Pipe is also given Read and Write rights to the general user. In addition, the service program does not verify the user when communicating. A thread may exist with a specific command. When the path of the program to be executed is sent, there is a local privilege escalation in which the service program executes the path with system privileges.	7.8	More Details
CVE-2020-14111	A command injection vulnerability exists in the Xiaomi Router AX3600. The vulnerability is caused by a lack of inspection for incoming data detection. Attackers can exploit this vulnerability to execute code.	7.8	More Details
CVE-2022-21124	Out-of-bounds write vulnerability in CX-Programmer v9.76.1 and earlier which is a part of CX-One (v4.60) suite allows an attacker to cause information disclosure and/or arbitrary code execution by having a user to open a specially crafted CXP file. This vulnerability is different from CVE-2022-25234.	7.8	More Details
CVE-2022-20048	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917502; Issue ID: ALPS05917502.	7.8	More Details
CVE-2022-20047	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917489; Issue ID: ALPS05917489.	7.8	More Details
CVE-2022-24286	Acer QuickAccess 2.01.300x before 2.01.3030 and 3.00.30xx before 3.00.3038 contains a local privilege escalation vulnerability. The user process communicates with a service of system authority through a named pipe. In this case, the Named Pipe is also given Read and Write rights to the general user. In addition, the service program does not verify the user when communicating. A thread may exist with a specific command. When the path of the program to be executed is sent, there is a local privilege escalation in which the service program executes the path with system privileges.	7.8	More Details
CVE-2022-23731	V8 javascript engine (heap vulnerability) can cause privilege escalation ,which can impact on some webOS TV models.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21219	Out-of-bounds read vulnerability in CX-Programmer v9.76.1 and earlier which is a part of CX-One (v4.60) suite allows an attacker to cause information disclosure and/or arbitrary code execution by having a user to open a specially crafted CXP file.	7.8	More Details
CVE-2022-24396	The Simple Diagnostics Agent - versions 1.0 up to version 1.57, does not perform any authentication checks for functionalities that can be accessed via localhost on http port 3005. Due to lack of authentication checks, an attacker could access administrative or other privileged functionalities and read, modify, or delete sensitive information and configurations.	7.8	More Details
CVE-2022-0847	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system.	7.8	More Details
CVE-2021-40376	otris Update Manager 1.2.1.0 allows local users to achieve SYSTEM access via unauthenticated calls to exposed interfaces over a .NET named pipe. A remote attack may be possible as well, by leveraging WsHTTPBinding for HTTP traffic on TCP port 9000.	7.8	More Details
CVE-2022-0516	A vulnerability was found in kvm_s390_guest_sida_op in the arch/s390/kvm/kvm-s390.c function in KVM for s390 in the Linux kernel. This flaw allows a local attacker with a normal user privilege to obtain unauthorized memory write access. This flaw affects Linux kernel versions prior to 5.17-rc4.	7.8	More Details
CVE-2022-24618	Heimdal.Wizard.exe installer in Heimdal Premium Security 2.5.395 and earlier has insecure permissions, which allows unprivileged local users to elevate privileges to SYSTEM via the "Browse For Folder" window accessible by triggering a "Repair" on the MSI package located in C:\Windows\Installer.	7.8	More Details
CVE-2022-23187	Adobe Illustrator version 26.0.3 (and earlier) is affected by a buffer overflow vulnerability due to insecure handling of a crafted file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file in Illustrator.	7.8	More Details
CVE-2021-33658	atune before 0.3-0.8 log in as a local user and run the curl command to access the local atune url interface to escalate the local privilege or modify any file. Authentication is not forcibly enabled in the default configuration.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23401	The following Yokogawa Electric products contain insecure DLL loading issues. CENTUM CS 3000 versions from R3.08.10 to R3.09.00, CENTUM VP versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, and from R6.01.00 to R6.08.00, Exaopc versions from R3.72.00 to R3.79.00.	7.8	More Details
CVE-2022-22148	'Root Service' service implemented in the following Yokogawa Electric products creates some named pipe with improper ACL configuration. CENTUM CS 3000 versions from R3.08.10 to R3.09.00, CENTUM VP versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, and from R6.01.00 to R6.08.00, Exaopc versions from R3.72.00 to R3.79.00.	7.8	More Details
CVE-2022-25217	Use of a hard-coded cryptographic key pair by the telnetd_startup service allows an attacker on the local area network to obtain a root shell on the device over telnet. The builds of telnetd_startup included in the version 22.5.9.163 of the K2 firmware, and version 32.1.15.93 of the K3C firmware (possibly amongst many other releases) included both the private and public RSA keys. The remaining versions cited here redacted the private key, but left the public key unchanged. An attacker in possession of the leaked private key may, through a scripted exchange of UDP packets, instruct telnetd_startup to spawn an unauthenticated telnet shell as root, by means of which they can then obtain complete control of the device. A consequence of the limited availablility of firmware images for testing is that models and versions not listed here may share this vulnerability.	7.8	More Details
CVE-2022-22141	'Long-term Data Archive Package' service implemented in the following Yokogawa Electric products creates some named pipe with imporper ACL configuration. CENTUM CS 3000 versions from R3.08.10 to R3.09.00, CENTUM VP versions from R4.01.00 to R4.03.00, from R5.01.00 to R5.04.20, and from R6.01.00 to R6.08.00, Exaopc versions from R3.72.00 to R3.79.00.	7.8	More Details
CVE-2022-25230	Use after free vulnerability in CX-Programmer v9.76.1 and earlier which is a part of CX-One (v4.60) suite allows an attacker to cause information disclosure and/or arbitrary code execution by having a user to open a specially crafted CXP file. This vulnerability is different from CVE-2022-25325.	7.8	More Details
CVE-2022-25234	Out-of-bounds write vulnerability in CX-Programmer v9.76.1 and earlier which is a part of CX-One (v4.60) suite allows an attacker to cause information disclosure and/or arbitrary code execution by having a user to open a specially crafted CXP file. This vulnerability is different from CVE-2022-21124.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25294	Proofpoint Insider Threat Management Agent for Windows relies on an inherently dangerous function that could enable an unprivileged local Windows user to run arbitrary code with SYSTEM privileges. All versions prior to 7.12.1 are affected. Agents for MacOS and Linux and Cloud are unaffected. Proofpoint has released fixed software version 7.12.1. The fixed software versions are available through the customer support portal.	7.8	More Details
CVE-2022-25325	Use after free vulnerability in CX-Programmer v9.76.1 and earlier which is a part of CX-One (v4.60) suite allows an attacker to cause information disclosure and/or arbitrary code execution by having a user to open a specially crafted CXP file. This vulnerability is different from CVE-2022-25230.	7.8	More Details
CVE-2021-42855	It was discovered that the SteelCentral AppInternals Dynamic Sampling Agent (DSA) uses the ".debug_command.config" file to store a json string that contains a list of IDs and pre-configured commands. The config file is subsequently used by the "/api/appInternals/1.0/agent/configuration" API to map the corresponding ID to a command to be executed.	7.8	More Details
CVE-2021-32025	An elevation of privilege vulnerability in the QNX Neutrino Kernel of affected versions of QNX Software Development Platform version(s) 6.4.0 to 7.0, QNX Momentics all 6.3.x versions, QNX OS for Safety versions 1.0.0 to 1.0.2, QNX OS for Safety versions 2.0.0 to 2.0.1, QNX for Medical versions 1.0.0 to 1.1.1, and QNX OS for Medical version 2.0.0 could allow an attacker to potentially access data, modify behavior, or permanently crash the system.	7.8	More Details
CVE-2022-25943	The installer of WPS Office for Windows versions prior to v11.2.0.10258 fails to configure properly the ACL for the directory where the service program is installed.	7.8	More Details
CVE-2022-20054	In ims service, there is a possible AT command injection due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219083; Issue ID: ALPS06219083.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20001	fish is a command line shell. fish version 3.1.0 through version 3.3.1 is vulnerable to arbitrary code execution. git repositories can contain per-repository configuration that change the behavior of git, including running arbitrary commands. When using the default configuration of fish, changing to a directory automatically runs `git` commands in order to display information about the current repository in the prompt. If an attacker can convince a user to change their current directory into one controlled by the attacker, such as on a shared file system or extracted archive, fish will run arbitrary commands under the attacker's control. This problem has been fixed in fish 3.4.0. Note that running git in these directories, including using the git tab completion, remains a potential trigger for this issue. As a workaround, remove the `fish_git_prompt` function from the prompt.	7.8	More Details
CVE-2022-24501	VP9 Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-23295	Raw Image Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-23296	Windows Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24577	GPAC 1.0.1 is affected by a NULL pointer dereference in gf_utf8_wcslen. (gf_utf8_wcslen is a renamed Unicode utf8_wcslen function.)	7.8	More Details
CVE-2022-23299	Windows PDEV Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-23300	Raw Image Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-23301	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-24451	VP9 Video Extensions Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24578	GPAC 1.0.1 is affected by a heap-based buffer overflow in SFS_AddString () at bifs/script_dec.c.	7.8	More Details
CVE-2022-24507	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-0943	Heap-based Buffer Overflow occurs in vim in GitHub repository vim/vim prior to 8.2.4563.	7.8	More Details
CVE-2022-24452	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-24453	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-24454	Windows Security Support Provider Interface Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24455	Windows CD-ROM Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24456	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-24457	HEIF Image Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-24459	Windows Fax and Scan Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24575	GPAC 1.0.1 is affected by a stack-based buffer overflow through MP4Box.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24509	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-24461	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-41850	An issue was discovered in Luna Simo PPR1.180610.011/202001031830. A pre-installed app with a package name of com.skyroam.silverhelper writes three IMEI values to system properties at system startup. The system property values can be obtained via getprop by all third-party applications co-located on the device, even those with no permissions granted, exposing the IMEI values to processes without enforcing any access control.	7.8	More Details
CVE-2022-24094	Adobe After Effects versions 22.2 (and earlier) and 18.4.4 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-24095	Adobe After Effects versions 22.2 (and earlier) and 18.4.4 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-24096	Adobe After Effects versions 22.2 (and earlier) and 18.4.4 (and earlier) are affected by an Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-24097	Adobe After Effects versions 22.2 (and earlier) and 18.4.4 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-25486	CuppaCMS v1.0 was discovered to contain a local file inclusion via the url parameter in /alerts/alertConfigField.php.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41848	An issue was discovered in Luna Simo PPR1.180610.011/202001031830. It mishandles software updates such that local third-party apps can provide a spoofed software update file that contains an arbitrary shell script and arbitrary ARM binary, where both will be executed as the root user with an SELinux domain named osi. To exploit this vulnerability, a local third-party app needs to have write access to external storage to write the spoofed update at the expected path. The vulnerable system binary (i.e., /system/bin/osi_bin) does not perform any authentication of the update file beyond ensuring that it is encrypted with an AES key (that is hard-coded in the vulnerable system binary). Processes executing with the osi SELinux domain can programmatically perform the following actions: install apps, grant runtime permissions to apps (including permissions with protection levels of dangerous and development), access extensive Personally Identifiable Information (PII) using the programmatically grant permissions, uninstall apps, set the default launcher app to a malicious launcher app that spoofs other apps, set a network proxy to intercept network traffic, unload kernel modules, set the default keyboard to a keyboard that has keylogging functionality, examine notification contents, send text messages, and more. The spoofed update can optionally contain an arbitrary ARM binary that will be locally stored in internal storage and executed at system startup to achieve persistent code execution as the root user with the osi SELinux domain. This ARM binary will continue to execute at startup even if the app that provided the spoofed update is uninstalled.	7.8	More Details
CVE-2022-25485	CuppaCMS v1.0 was discovered to contain a local file inclusion via the url parameter in /alerts/alertLightbox.php.	7.8	More Details
CVE-2022-22006	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-22007	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-24510	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-23266	Microsoft Defender for IoT Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23282	Paint 3D Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-26967	GPAC 2.0 allows a heap-based buffer overflow in gf_base64_encode. It can be triggered via MP4Box.	7.8	More Details
CVE-2022-23290	Windows Inking COM Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-23291	Windows DWM Core Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-24696	Mirametrix Glance before 5.1.1.42207 (released on 2018-08-30) allows a local attacker to elevate privileges. NOTE: this is unrelated to products from the glance.com and glance.net websites.	7.8	More Details
CVE-2022-26981	Liblouis through 3.21.0 has a buffer overflow in compilePassOpcode in compileTranslationTable.c (called, indirectly, by tools/lou_checktable.c).	7.8	More Details
CVE-2022-23293	Windows Fast FAT File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-20053	In ims service, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219097; Issue ID: ALPS06219097.	7.8	More Details
CVE-2022-24753	Stripe CLI is a command-line tool for the Stripe eCommerce platform. A vulnerability in Stripe CLI exists on Windows when certain commands are run in a directory where an attacker has planted files. The commands are \`stripe login\`, \`stripe config -e\`, \`stripe community\`, and \`stripe open\`. MacOS and Linux are unaffected. An attacker who successfully exploits the vulnerability can run arbitrary code in the context of the current user. The update addresses the vulnerability by throwing an error in these situations before the code can run.Users are advised to upgrade to version 1.7.13. There are no known workarounds for this issue.	7.7	More Details
CVE-2022-0908	Null source pointer passed as an argument to memcpy() function within TIFFFetchNormalTag () in tif_dirread.c in libtiff versions up to 4.3.0 could lead to Denial of Service via crafted TIFF file.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21819	NVIDIA distributions of Jetson Linux contain a vulnerability where an error in the IOMMU configuration may allow an unprivileged attacker with physical access to the board direct read/write access to the entire system address space through the PCI bus. Such an attack could result in denial of service, code execution, escalation of privileges, and impact to data integrity and confidentiality. The scope impact may extend to other components.	7.6	More Details
CVE-2022-25554	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the deviceId parameter.	7.5	More Details
CVE-2022-26779	Apache CloudStack prior to 4.16.1.0 used insecure random number generation for project invitation tokens. If a project invite is created based only on an email address, a random token is generated. An attacker with knowledge of the project ID and the fact that the invite is sent, could generate time deterministic tokens and brute force attempt to use them prior to the legitimate receiver accepting the invite. This feature is not enabled by default, the attacker is required to know or guess the project ID for the invite in addition to the invitation token, and the attacker would need to be an existing authorized user of CloudStack.	7.5	More Details
CVE-2020-36518	jackson-databind before 2.13.0 allows a Java StackOverflow exception and denial of service via a large depth of nested objects.	7.5	More Details
CVE-2022-22719	A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.	7.5	More Details
CVE-2022-0913	Integer Overflow or Wraparound in GitHub repository microweber/microweber prior to 1.3.	7.5	More Details
CVE-2022-24601	Luocms v2.0 is affected by SQL Injection in /admin/manager/admin_mod.php. An attacker can obtain sensitive information through SQL injection statements.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24756	Bareos is open source software for backup, archiving, and recovery of data for operating systems. When Bareos Director >= 18.2 but prior to 21.1.0, 20.0.6, and 19.2.12 is built and configured for PAM authentication, a failed PAM authentication will leak a small amount of memory. An attacker that is able to use the PAM Console (i.e. by knowing the shared secret or via the WebUI) can flood the Director with failing login attempts which will eventually lead to an out-of-memory condition in which the Director will not work anymore. Bareos Director versions 21.1.0, 20.0.6 and 19.2.12 contain a Bugfix for this problem. Users who are unable to upgrade may disable PAM authentication as a workaround.	7.5	More Details
CVE-2021-23246	In ACE2 ColorOS11, the attacker can obtain the foreground package name through permission promotion, resulting in user information disclosure.	7.5	More Details
CVE-2022-0778	The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25553	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsPwd parameter.	7.5	More Details
CVE-2021-32476	A denial-of-service risk was identified in the draft files area, due to it not respecting user file upload limits. Moodle versions 3.10 to 3.10.3, 3.9 to 3.9.6, 3.8 to 3.8.8, 3.5 to 3.5.17 and earlier unsupported versions are affected.	7.5	More Details
CVE-2021-42577	An issue was discovered in Softing OPC UA C++ SDK before 5.70. A malformed OPC/UA message abort packet makes the client crash with a NULL pointer dereference.	7.5	More Details
CVE-2022-0853	A flaw was found in JBoss-client. The vulnerability occurs due to a memory leak on the JBoss client-side, when using UserTransaction repeatedly and leads to information leakage vulnerability.	7.5	More Details
CVE-2022-22547	Simple Diagnostics Agent - versions 1.0 (up to version 1.57.), allows an attacker to access information which would otherwise be restricted via a random port 9000-65535. This allows information gathering which could be used exploit future open-source security exploits.	7.5	More Details
CVE-2022-25216	An absolute path traversal vulnerability allows a remote attacker to download any file on the Windows file system for which the user account running DVDFab 12 Player (recently renamed PlayerFab) has read-access, by means of an HTTP GET request to http://<IP_ADDRESS>:32080/download/<URL_ENCODED_PATH>.	7.5	More Details
CVE-2022-25491	HMS v1.0 was discovered to contain a SQL injection vulnerability via the editid parameter in appointment.php.	7.5	More Details
CVE-2021-45848	Denial of service (DoS) vulnerability in Nicotine+ 3.0.3 and later allows a user with a modified Soulseek client to crash Nicotine+ by sending a file download request with a file path containing a null character.	7.5	More Details
CVE-2022-25512	FreeTAKServer-UI v1.9.8 was discovered to leak sensitive API and Websocket keys.	7.5	More Details
CVE-2022-25508	An access control issue in the component /ManageRoute/postRoute of FreeTAKServer v1.9.8 allows unauthenticated attackers to cause a Denial of Service (DoS) via an unusually large amount of created routes, or create unsafe or false routes for legitimate users.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0280	A race condition vulnerability exists in the QuickClean feature of McAfee Total Protection for Windows prior to 16.0.43 that allows a local user to gain privilege elevation and perform an arbitrary file delete. This could lead to sensitive files being deleted and potentially cause denial of service. This attack exploits the way symlinks are created and how the product works with them.	7.5	More Details
CVE-2022-25557	Tenda AX1806 v1.0.0.1 was discovered to contain a heap overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the urls parameter.	7.5	More Details
CVE-2022-25552	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function form_fast_setting_wifi_set. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ssid parameter.	7.5	More Details
CVE-2022-25551	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsDomain parameter.	7.5	More Details
CVE-2022-25550	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the deviceName parameter.	7.5	More Details
CVE-2022-25549	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsEn parameter.	7.5	More Details
CVE-2022-25555	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ntpServer parameter.	7.5	More Details
CVE-2022-25548	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the serverName parameter.	7.5	More Details
CVE-2022-25547	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the time parameter.	7.5	More Details
CVE-2022-25546	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetSysToolDDNS. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ddnsUser parameter.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22354	IBM Spectrum Protect Plus 10.1.0.0 through 10.1.9.2 and IBM Spectrum Copy Data Management 2.2.0.0 through 2.2.14.3 do not limit the length of a connection which could allow for a Slowloris HTTP denial of service attack to take place. This can cause the Admin Console to become unresponsive. IBM X-Force ID: 220485.	7.5	More Details
CVE-2022-25558	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function formSetProvince. This vulnerability allows attackers to cause a Denial of Service (DoS) via the ProvinceCode parameter.	7.5	More Details
CVE-2022-25560	Tenda AX12 v22.03.01.21 was discovered to contain a stack overflow in the function sub_4327CC. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter.	7.5	More Details
CVE-2022-25561	Tenda AX12 v22.03.01.21 was discovered to contain a stack overflow in the function sub_42DE00. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter.	7.5	More Details
CVE-2022-25566	Tenda AX1806 v1.0.0.1 was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the time parameter.	7.5	More Details
CVE-2022-26311	Couchbase Operator 2.2.x before 2.2.3 exposes Sensitive Information to an Unauthorized Actor. Secrets are not redacted in logs collected from Kubernetes environments.	7.5	More Details
CVE-2022-26662	An XML Entity Expansion (XEE) issue was discovered in Tryton Application Platform (Server) 5.x through 5.0.45, 6.x through 6.0.15, and 6.1.x and 6.2.x through 6.2.5, and Tryton Application Platform (Command Line Client (proteus)) 5.x through 5.0.11, 6.x through 6.0.4, and 6.1.x and 6.2.x through 6.2.1. An unauthenticated user can send a crafted XML-RPC message to consume all the resources of the server.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24726	Istio is an open platform to connect, manage, and secure microservices. In affected versions the Istio control plane, istiod, is vulnerable to a request processing error, allowing a malicious attacker that sends a specially crafted message which results in the control plane crashing when the validating webhook for a cluster is exposed publicly. This endpoint is served over TLS port 15017, but does not require any authentication from the attacker. For simple installations, Istiod is typically only reachable from within the cluster, limiting the blast radius. However, for some deployments, especially [external istiod] (https://istio.io/latest/docs/setup/install/external-controlplane/) topologies, this port is exposed over the public internet. This issue has been patched in versions 1.13.2, 1.12.5 and 1.11.8. Users are advised to upgrade. Users unable to upgrade should disable access to a validating webhook that is exposed to the public internet or restrict the set of IP addresses that can query it to a set of known, trusted entities.	7.5	More Details
CVE-2022-25556	Tenda AX12 v22.03.01.21 was discovered to contain a stack overflow in the function sub_42E328. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter.	7.5	More Details
CVE-2022-23989	In Stormshield Network Security (SNS) before 3.7.25, 3.8.x through 3.11.x before 3.11.13, 4.x before 4.2.10, and 4.3.x before 4.3.5, a flood of connections to the SSLVPN service might lead to saturation of the loopback interface. This could result in the blocking of almost all network traffic, making the firewall unreachable. An attacker could exploit this via forged and properly timed traffic to cause a denial of service.	7.5	More Details
CVE-2021-40057	There is a heap-based and stack-based buffer overflow vulnerability in the video framework. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2021-40052	There is an incorrect buffer size calculation vulnerability in the video framework.Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2021-44032	TP-Link Omada SDN Software Controller before 5.0.15 does not check if the authentication method specified in a connection request is allowed. An attacker can bypass the captive portal authentication process by using the downgraded "no authentication" method, and access the protected network. For example, the attacker can simply set window.authType=0 in client-side JavaScript.	7.5	More Details
CVE-2021-40064	There is a heap-based buffer overflow vulnerability in system components. Successful exploitation of this vulnerability may affect system stability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38296	Apache Spark supports end-to-end encryption of RPC connections via "spark.authenticate" and "spark.network.crypto.enabled". In versions 3.1.2 and earlier, it uses a bespoke mutual authentication protocol that allows for full encryption key recovery. After an initial interactive attack, this would allow someone to decrypt plaintext traffic offline. Note that this does not affect security mechanisms controlled by "spark.authenticate.enableSaslEncryption", "spark.io.encryption.enabled", "spark.ssl", "spark.ui.strictTransportSecurity". Update to Apache Spark 3.1.3 or later	7.5	More Details
CVE-2022-0618	A program using swift-nio-http2 is vulnerable to a denial of service attack, caused by a network peer sending a specially crafted HTTP/2 frame. This vulnerability is caused by a logical error when parsing a HTTP/2 HEADERS or HTTP/2 PUSH_PROMISE frame where the frame contains padding information without any other data. This logical error caused confusion about the size of the frame, leading to a parsing error. This parsing error immediately crashes the entire process. Sending a HEADERS frame or PUSH_PROMISE frame with HTTP/2 padding information does not require any special permission, so any HTTP/2 connection peer may send such a frame. For clients, this means any server to which they connect may launch this attack. For servers, anyone they allow to connect to them may launch such an attack. The attack is low-effort: it takes very little resources to send an appropriately crafted frame. The impact on availability is high: receiving the frame immediately crashes the server, dropping all in-flight connections and causing the service to need to restart. It is straightforward for an attacker to repeatedly send appropriately crafted frames, so attackers require very few resources to achieve a substantial denial of service. The attack does not have any confidentiality or integrity risks in and of itself: swift-nio-http2 is parsing the frame in memory-safe code, so the crash is safe. However, sudden process crashes can lead to violations of invariants in services, so it is possible that this attack can be used to trigger an error condition that has confidentiality or integrity risks. The risk can be mitigated if untrusted peers can be prevented from communicating with the service. This mitigation is not available to many services. The issue is fixed by rewriting the parsing code to correctly handle the condition. The issue was found by automated fuzzing by oss-fuzz.	7.5	More Details
CVE-2021-40063	There is an improper access control vulnerability in the video module. Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0725	A flaw was found in keepass. The vulnerability occurs due to logging the plain text passwords in system log and leads to an Information Exposure vulnerability. This flaw allows an attacker to interact and read sensitive passwords and logs.	7.5	More Details
CVE-2021-40062	There is a vulnerability of copying input buffer without checking its size in the video framework. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2021-40061	There is a vulnerability of accessing resources using an incompatible type (type confusion) in the Bastet module. Successful exploitation of this vulnerability may affect integrity.	7.5	More Details
CVE-2021-40060	There is a heap-based buffer overflow vulnerability in the video framework. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2021-40058	There is a heap-based buffer overflow vulnerability in the video framework. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2020-36517	An information leak in Nabu Casa Home Assistant Operating System and Home Assistant Supervised 2022.03 allows a DNS operator to gain knowledge about internal network resources via the hardcoded DNS resolver configuration.	7.5	More Details
CVE-2021-40054	There is an integer underflow vulnerability in the atcmdserver module. Successful exploitation of this vulnerability may affect integrity.	7.5	More Details
CVE-2021-40056	There is a vulnerability of copying input buffer without checking its size in the video framework. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2021-40051	There is an unauthorized access vulnerability in system components. Successful exploitation of this vulnerability will affect confidentiality.	7.5	More Details
CVE-2021-40049	There is a permission control vulnerability in the PMS module. Successful exploitation of this vulnerability can lead to sensitive system information being obtained without authorization.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3698	A flaw was found in Cockpit in versions prior to 260 in the way it handles the certificate verification performed by the System Security Services Daemon (SSSD). This flaw allows client certificates to authenticate successfully, regardless of the Certificate Revocation List (CRL) configuration or the certificate status. The highest threat from this vulnerability is to confidentiality.	7.5	More Details
CVE-2021-40047	There is a vulnerability of memory not being released after effective lifetime in the Bastet module. Successful exploitation of this vulnerability may affect integrity.	7.5	More Details
CVE-2021-40048	There is an incorrect buffer size calculation vulnerability in the video framework. Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2021-46408	Tenda AX12 v22.03.01.21 was discovered to contain a stack buffer overflow in the function sub_422CE4. This vulnerability allows attackers to cause a Denial of Service (DoS) via the strcpy parameter.	7.5	More Details
CVE-2022-24464	.NET and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2022-25214	Improper access control on the LocalClientList.asp interface allows an unauthenticated remote attacker to obtain sensitive information concerning devices on the local area network, including IP and MAC addresses. Improper access control on the wirelesssetup.asp interface allows an unauthenticated remote attacker to obtain the WPA passphrases for the 2.4GHz and 5.0GHz wireless networks. This is particularly dangerous given that the K2G setup wizard presents the user with the option of using the same password for the 2.4Ghz network and the administrative interface, by clicking a checkbox. When Remote Managment is enabled, these endpoints are exposed to the WAN.	7.4	More Details
CVE-2022-24467	Azure Site Recovery Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-24468	Azure Site Recovery Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-0944	Template injection in connection test endpoint leads to RCE in GitHub repository sqlpad/sqlpad prior to 6.10.1.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24471	Azure Site Recovery Remote Code Execution Vulnerability	7.2	More Details
CVE-2021-42171	Zenario CMS 9.0.54156 is vulnerable to File Upload. The web server can be compromised by uploading and executing a web-shell which can run commands, browse system files, browse local resources, attack other servers, and exploit the local vulnerabilities, and so forth.	7.2	More Details
CVE-2022-23284	Windows Print Spooler Elevation of Privilege Vulnerability	7.2	More Details
CVE-2021-32474	An SQL injection risk existed on sites with MNet enabled and configured, via an XML-RPC call from the connected peer host. Note that this required site administrator access or access to the keypair. Moodle 3.10 to 3.10.3, 3.9 to 3.9.6, 3.8 to 3.8.8, 3.5 to 3.5.17 and earlier unsupported versions are affected.	7.2	More Details
CVE-2022-25225	Network Olympus version 1.8.0 allows an authenticated admin user to inject SQL queries in '/api/eventinstance' via the 'sqlparameter' JSON parameter. It is also possible to achieve remote code execution in the default installation (PostgreSQL) by exploiting this issue.	7.2	More Details
CVE-2022-24517	Azure Site Recovery Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-23265	Microsoft Defender for IoT Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-24470	Azure Site Recovery Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-26521	Abantecart through 1.3.2 allows remote authenticated administrators to execute arbitrary code by uploading an executable file, because the Catalog>Media Manager>Images settings can be changed by an administrator (e.g., by configuring .php to be a valid image file type).	7.2	More Details
CVE-2022-24520	Azure Site Recovery Remote Code Execution Vulnerability	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24734	MyBB is a free and open source forum software. In affected versions the Admin CP's Settings management module does not validate setting types correctly on insertion and update, making it possible to add settings of supported type `php` with PHP code, executed on on _Change Settings_ pages. This results in a Remote Code Execution (RCE) vulnerability. The vulnerable module requires Admin CP access with the `Can manage settings?` permission. MyBB's Settings module, which allows administrators to add, edit, and delete non-default settings, stores setting data in an options code string ($options_code; mybb_settings.optionscode database column) that identifies the setting type and its options, separated by a new line character (\n). In MyBB 1.2.0, support for setting type php was added, for which the remaining part of the options code is PHP code executed on Change Settings pages (reserved for plugins and internal use). MyBB 1.8.30 resolves this issue. There are no known workarounds.	7.2	More Details
CVE-2022-24743	Sylius is an open source eCommerce platform. Prior to versions 1.10.11 and 1.11.2, the reset password token was not set to null after the password was changed. The same token could be used several times, which could result in leak of the existing token and unauthorized password change. The issue is fixed in versions 1.10.11 and 1.11.2. As a workaround, overwrite the `Sylius\Bundle\ApiBundle\CommandHandler\ResetPasswordHandler` class with code provided by the maintainers and register it in a container. More information about this workaround is available in the GitHub Security Advisory.	7.1	More Details
CVE-2022-0905	Missing Authorization in GitHub repository go-gitea/gitea prior to 1.16.4.	7.1	More Details
CVE-2021-3739	A NULL pointer dereference flaw was found in the btrfs_rm_device function in fs/btrfs/volumes.c in the Linux Kernel, where triggering the bug requires ‘CAP_SYS_ADMIN’. This flaw allows a local attacker to crash the system or leak kernel internal information. The highest threat from this vulnerability is to system availability.	7.1	More Details
CVE-2022-24505	Windows ALPC Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-23287	Windows ALPC Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23286	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-23040	Linux PV device frontends vulnerable to attacks by backends T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend. CVE-2022-23042	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23039	Linux PV device frontends vulnerable to attacks by backends T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend. CVE-2022-23042	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23038	Linux PV device frontends vulnerable to attacks by backends T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend. CVE-2022-23042	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23037	Linux PV device frontends vulnerable to attacks by backends T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend. CVE-2022-23042	7.0	More Details
CVE-2022-23283	Windows ALPC Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23036	Linux PV device frontends vulnerable to attacks by backends T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend. CVE-2022-23042	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23041	Linux PV device frontends vulnerable to attacks by backends T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend. CVE-2022-23042	7.0	More Details
CVE-2022-23288	Windows DWM Core Library Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-26488	In Python before 3.10.3 on Windows, local users can gain privileges because the search path is inadequately secured. The installer may allow a local attacker to add user-writable directories to the system search path. To exploit, an administrator must have installed Python for all users and enabled PATH entries. A non-administrative user can trigger a repair that incorrectly adds user-writable paths into PATH, enabling search-path hijacking of other users and system services. This affects Python (CPython) through 3.7.12, 3.8.x through 3.8.12, 3.9.x through 3.9.10, and 3.10.x through 3.10.2.	7.0	More Details
CVE-2022-23298	Windows NT OS Kernel Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24460	Tablet Windows User Interface Application Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-21967	Xbox Live Auth Manager for Windows Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-24525	Windows Update Stack Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-23042	Linux PV device frontends vulnerable to attacks by backends T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend. CVE-2022-23042	7.0	More Details
CVE-2022-22795	Signiant - Manager+Agents XML External Entity (XXE) - Extract internal files of the affected machine An attacker can read all the system files, the product is running with root on Linux systems and nt/authority on windows systems, which allows him to access and extract any file on the systems, such as passwd, shadow, hosts and so on. By gaining access to these files, attackers can steal sensitive information from the victims machine.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24748	Shopware is an open commerce platform based on the Symfony php Framework and the Vue javascript framework. In versions prior to 6.4.8.2 it is possible to modify customers and to create orders without App Permission. This issue is a result of improper api route checking. Users are advised to upgrade to version 6.4.8.2. There are no known workarounds.	6.8	More Details
CVE-2021-33150	Hardware allows activation of test or debug logic at runtime for some Intel(R) Trace Hub instances which may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2022-20055	In preloader (usb), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160830.	6.8	More Details
CVE-2022-25213	Improper physical access control and use of hard-coded credentials in /etc/passwd permits an attacker with physical access to obtain a root shell via an unprotected UART port on the device. The same port exposes an unauthenticated Das U-Boot BIOS shell.	6.8	More Details
CVE-2022-20050	In connsyslogger, there is a possible symbolic link following due to improper link resolution. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06335038; Issue ID: ALPS06335038.	6.7	More Details
CVE-2022-20049	In vpu, there is a possible escalation of privilege due to a missing permission check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05954679; Issue ID: ALPS05954679.	6.7	More Details
CVE-2022-0921	Abusing Backup/Restore feature to achieve Remote Code Execution in GitHub repository microweber/microweber prior to 1.2.12.	6.7	More Details
CVE-2022-20060	In preloader (usb), there is a possible permission bypass due to a missing proper image authentication. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06137462.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20059	In preloader (usb), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160781.	6.6	More Details
CVE-2022-20058	In preloader (usb), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160485.	6.6	More Details
CVE-2022-20056	In preloader (usb), there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, for an attacker who has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160820.	6.6	More Details
CVE-2022-0593	The Login with phone number WordPress plugin before 1.3.7 includes a file delete.php with no form of authentication or authorization checks placed in the plugin directory, allowing unauthenticated user to remotely delete the plugin files leading to a potential Denial of Service situation.	6.5	More Details
CVE-2022-25506	FreeTAKServer-UI v1.9.8 was discovered to contain a SQL injection vulnerability via the API endpoint /AuthenticateUser.	6.5	More Details
CVE-2021-34338	Ming 0.4.8 has an out-of-bounds buffer overwrite issue in the function getName() in decompiler.c file that causes a direct segmentation fault and leads to denial of service.	6.5	More Details
CVE-2022-21132	Directory traversal vulnerability in pfSense-pkg-WireGuard pfSense-pkg-WireGuard 0.1.5 versions prior to 0.1.5_4 and pfSense-pkg-WireGuard 0.1.6 versions prior to 0.1.6_1 allows a remote authenticated attacker to lead a pfSense user to view a file outside the public folder.	6.5	More Details
CVE-2021-34339	Ming 0.4.8 has an out-of-bounds buffer access issue in the function getString() in decompiler.c file that causes a direct segmentation fault and leads to denial of service.	6.5	More Details
CVE-2022-25511	An issue in the ?filename= argument of the route /DataPackageTable in FreeTAKServer-UI v1.9.8 allows attackers to place arbitrary files anywhere on the system.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34340	Ming 0.4.8 has an out-of-bounds buffer access issue in the function decompileINCR_DECR() in decompiler.c file that causes a direct segmentation fault and leads to denial of service.	6.5	More Details
CVE-2022-22353	IBM Big SQL on IBM Cloud Pak for Data 7.1.0, 7.1.1, 7.2.0, and 7.2.3 could allow an authenticated user with appropriate permissions to obtain sensitive information by bypassing data masking rules using a CREATE TABLE SELECT statement. IBM X-Force ID: 220480.	6.5	More Details
CVE-2022-0881	Insecure Storage of Sensitive Information in GitHub repository chocobozzz/peertube prior to 4.1.1.	6.5	More Details
CVE-2021-41233	Nextcloud text is a collaborative document editing using Markdown built for the nextcloud server. Due to an issue with the Nextcloud Text application, which is by default shipped with Nextcloud Server, an attacker is able to access the folder names of "File Drop". For successful exploitation an attacker requires knowledge of the sharing link. It is recommended that users upgrade their Nextcloud Server to 20.0.14, 21.0.6 or 22.2.1. Users unable to upgrade should disable the Nextcloud Text application in the application settings.	6.5	More Details
CVE-2021-26341	Some AMD CPUs may transiently execute beyond unconditional direct branches, which may potentially result in data leakage.	6.5	More Details
CVE-2022-0821	Improper Authorization in GitHub repository orchardcms/orchardcore prior to 1.3.0.	6.5	More Details
CVE-2022-26652	NATS nats-server before 2.7.4 allows Directory Traversal (with write access) via an element in a ZIP archive for JetStream streams. nats-streaming-server before 0.24.3 is also affected.	6.5	More Details
CVE-2021-32436	An out-of-bounds read in the function write_title() in subs.c of abcm2ps v8.14.11 allows remote attackers to cause a Denial of Service (DoS) via unspecified vectors.	6.5	More Details
CVE-2021-39051	IBM Spectrum Copy Data Management 2.2.0.0 through 2.2.14.3 is vulnerable to server-side request forgery, caused by improper input of application server registration function. A remote attacker could exploit this vulnerability using the host address and port fields of the application server registration form in the portal UI to enumerate and attack services that are running on those hosts. IBM X-Force ID: 214441.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0815	Improper access control vulnerability in McAfee WebAdvisor Chrome and Edge browser extensions up to 8.1.0.1895 allows a remote attacker to gain access to McAfee WebAdvisor settings and other details about the user’s system. This could lead to unexpected behaviors including; settings being changed, fingerprinting of the system leading to targeted scams, and not triggering the malicious software if McAfee software is detected.	6.5	More Details
CVE-2022-20057	In btif, there is a possible memory corruption due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06271186; Issue ID: ALPS06271186.	6.5	More Details
CVE-2021-3733	There's a flaw in urllib's AbstractBasicAuthHandler class. An attacker who controls a malicious HTTP server that an HTTP client (such as web browser) connects to, could trigger a Regular Expression Denial of Service (ReDOS) during an authentication request with a specially crafted payload that is sent by the server to the client. The greatest threat that this flaw poses is to application availability.	6.5	More Details
CVE-2022-0932	Missing Authorization in GitHub repository saleor/saleor prior to 3.1.2.	6.5	More Details
CVE-2022-24463	Microsoft Exchange Server Spoofing Vulnerability	6.5	More Details
CVE-2022-26661	An XXE issue was discovered in Tryton Application Platform (Server) 5.x through 5.0.45, 6.x through 6.0.15, and 6.1.x and 6.2.x through 6.2.5, and Tryton Application Platform (Command Line Client (proteus)) 5.x through 5.0.11, 6.x through 6.0.4, and 6.1.x and 6.2.x through 6.2.1. An authenticated user can make the server parse a crafted XML SEPA file to access arbitrary files on the system.	6.5	More Details
CVE-2022-27203	Jenkins Extended Choice Parameter Plugin 346.vd87693c5a_86c and earlier allows attackers with Item/Configure permission to read values from arbitrary JSON and Java properties files on the Jenkins controller.	6.5	More Details
CVE-2021-24692	The Simple Download Monitor WordPress plugin before 3.9.5 allows users with a role as low as Contributor to download any file on the web server (such as wp-config.php) via a path traversal vector.	6.5	More Details
CVE-2022-27210	A cross-site request forgery (CSRF) vulnerability in Jenkins Kubernetes Continuous Deploy Plugin 2.3.1 and earlier allows attackers to connect to an attacker-specified SSH server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27211	A missing permission check in Jenkins Kubernetes Continuous Deploy Plugin 2.3.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified SSH server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2022-24398	Under certain conditions SAP Business Objects Business Intelligence Platform - versions 420, 430, allows an authenticated attacker to access information which would otherwise be restricted.	6.5	More Details
CVE-2021-28488	Ericsson Network Manager (ENM) before 21.2 has incorrect access-control behavior (that only affects the level of access available to persons who were already granted a highly privileged role). Users in the same AMOS authorization group can retrieve managed-network data that was not set to be accessible to the entire group (i.e., was only set to be accessible to a subset of that group).	6.5	More Details
CVE-2022-24515	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2021-43969	The login.jsp page of Quicklert for Digium 10.0.0 (1043) is affected by both Blind SQL Injection with Out-of-Band Interaction (DNS) and Blind Time-Based SQL Injections. Exploitation can be used to disclose all data within the database (up to and including the administrative accounts' login IDs and passwords) via the login.jsp uname parameter.	6.5	More Details
CVE-2022-25244	Vault Enterprise clusters using the tokenization transform feature can expose the tokenization key through the tokenization key configuration endpoint to authorized operators with `read` permissions on this endpoint. Fixed in Vault Enterprise 1.9.4, 1.8.9 and 1.7.10.	6.5	More Details
CVE-2022-25243	"Vault and Vault Enterprise 1.8.0 through 1.8.8, and 1.9.3 allowed the PKI secrets engine under certain configurations to issue wildcard certificates to authorized users for a specified domain, even if the PKI role policy attribute allow_subdomains is set to false. Fixed in Vault Enterprise 1.8.9 and 1.9.4.	6.5	More Details
CVE-2022-24519	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-24506	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24518	Azure Site Recovery Elevation of Privilege Vulnerability	6.5	More Details
CVE-2022-27209	A missing permission check in Jenkins Kubernetes Continuous Deploy Plugin 2.3.1 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	6.5	More Details
CVE-2022-27208	Jenkins Kubernetes Continuous Deploy Plugin 2.3.1 and earlier allows users with Credentials/Create permission to read arbitrary files on the Jenkins controller.	6.5	More Details
CVE-2022-23625	Wire-ios is a messaging application using the wire protocol on apple's ios platform. In versions prior to 3.95 malformed resource identifiers may render the iOS Wire Client completely unusable by causing it to repeatedly crash on launch. These malformed resource identifiers can be generated and sent between Wire users. The root cause lies in [wireapp/wire-ios-transport](https://github.com/wireapp/wire-ios-transport), where code responsible for removing sensible tokens before logging may fail and lead to a crash (Swift exception) of the application. This causes undesirable behavior, however the (greater) Wire system is still functional. Users are advised to upgrade as soon as possible. There are no known workarounds for this issue.	6.5	More Details
CVE-2022-24960	A use after free vulnerability was discovered in PDFTron SDK version 9.2.0. A crafted PDF can overwrite RIP with data previously allocated on the heap. This issue affects: PDFTron PDFTron SDK 9.2.0 on OSX; 9.2.0 on Linux; 9.2.0 on Windows.	6.5	More Details
CVE-2022-23253	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability	6.5	More Details
CVE-2022-27206	Jenkins GitLab Authentication Plugin 1.13 and earlier stores the GitLab client secret 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-2022-0856	libcaca is affected by a Divide By Zero issue via img2txt, which allows a remote malicious user to cause a Denial of Service	6.5	More Details
CVE-2021-40059	There is a permission control vulnerability in the Wi-Fi module. Successful exploitation of this vulnerability may affect confidentiality.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27216	Jenkins dbCharts Plugin 0.5.2 and earlier stores JDBC connection passwords unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system.	6.5	More Details
CVE-2021-42262	An issue was discovered in Softing OPC UA C++ SDK before 5.70. An invalid XML element in the type dictionary makes the OPC/UA client crash due to an out-of-memory condition.	6.5	More Details
CVE-2022-24385	A Direct Object Access vulnerability in SmarterTools SmarterTrack leads to information disclosure This issue affects: SmarterTools SmarterTrack 100.0.8019.14010.	6.5	More Details
CVE-2022-27201	Jenkins Semantic Versioning Plugin 1.13 and earlier does not restrict execution of an controller/agent message to agents, and implements no limitations about the file path that can be parsed, allowing attackers able to control agent processes to have Jenkins parse a crafted file that uses external entities for extraction of secrets from the Jenkins controller or server-side request forgery.	6.5	More Details
CVE-2021-42389	Divide-by-zero in Clickhouse's Delta compression codec when parsing a malicious query. The first byte of the compressed buffer is used in a modulo operation without being checked for 0.	6.5	More Details
CVE-2021-42390	Divide-by-zero in Clickhouse's DeltaDouble compression codec when parsing a malicious query. The first byte of the compressed buffer is used in a modulo operation without being checked for 0.	6.5	More Details
CVE-2021-42391	Divide-by-zero in Clickhouse's Gorilla compression codec when parsing a malicious query. The first byte of the compressed buffer is used in a modulo operation without being checked for 0.	6.5	More Details
CVE-2022-25818	Improper boundary check in UWB stack prior to SMR Mar-2022 Release 1 allows arbitrary code execution.	6.5	More Details
CVE-2021-34342	Ming 0.4.8 has an out-of-bounds read vulnerability in the function newVar_N() in decompile.c which causes a huge information leak.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24762	sysend.js is a library that allows a user to send messages between pages that are open in the same browser. Users that use cross-origin communication may have their communications intercepted. Impact is limited by the communication occurring in the same browser. This issue has been patched in sysend.js version 1.10.0. The only currently known workaround is to avoid sending communications that a user does not want to have intercepted via sysend messages.	6.5	More Details
CVE-2022-0001	Non-transparent sharing of branch predictor selectors between contexts in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.	6.5	More Details
CVE-2022-0002	Non-transparent sharing of branch predictor within a context in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.	6.5	More Details
CVE-2022-27217	Jenkins Vmware vRealize CodeStream Plugin 1.2 and earlier stores passwords unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Extended Read permission, or access to the Jenkins controller file system.	6.5	More Details
CVE-2022-24522	Skype Extension for Chrome Information Disclosure Vulnerability	6.5	More Details
CVE-2021-32005	Cross-site Scripting (XSS) vulnerability in log view of Secomea SiteManager allows a logged in user to store javascript for later execution. This issue affects: Secomea SiteManager Version 9.6.621421014 and all prior versions.	6.5	More Details
CVE-2022-22835	An issue was discovered in OverIT Geocall before version 8.0. An authenticated user who has the Test Trasformazione XSL functionality enabled can exploit a XXE vulnerability to read arbitrary files from the filesystem.	6.5	More Details
CVE-2021-34341	Ming 0.4.8 has an out-of-bounds read vulnerability in the function decompileIF() in the decompile.c file that causes a direct segmentation fault and leads to denial of service.	6.5	More Details
CVE-2021-24982	The Child Theme Generator WordPress plugin through 2.2.7 does not sanitise escape the parade parameter before outputting it back, leading to a Reflected Cross-Site Scripting in the admin dashboard	6.4	More Details
CVE-2021-44750	An arbitrary code execution vulnerability was found in the F-Secure Support Tool. A standard user can craft a special configuration file, which when run by administrator can execute any commands.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44964	Use after free in garbage collector and finalizer of lgc.c in Lua interpreter 5.4.0~5.4.3 allows attackers to perform Sandbox Escape via a crafted script file.	6.3	More Details
CVE-2022-24512	.NET and Visual Studio Remote Code Execution Vulnerability	6.3	More Details
CVE-2022-24747	Shopware is an open commerce platform based on the Symfony php Framework and the Vue javascript framework. Affected versions of shopware do no properly set sensitive HTTP headers to be non-cacheable. If there is an HTTP cache between the server and client then headers may be exposed via HTTP caches. This issue has been resolved in version 6.4.8.2. There are no known workarounds.	6.3	More Details
CVE-2022-24732	Maddy Mail Server is an open source SMTP compatible email server. Versions of maddy prior to 0.5.4 do not implement password expiry or account expiry checking when authenticating using PAM. Users are advised to upgrade. Users unable to upgrade should manually remove expired accounts via existing filtering mechanisms.	6.3	More Details
CVE-2022-21146	Persistent cross-site scripting in the web interface of ipDIO allows an unauthenticated remote attacker to introduce arbitrary JavaScript by injecting an XSS payload into a specific parameter. The XSS payload will be executed when a legitimate user attempts to review history.	6.3	More Details
CVE-2022-25825	Improper access control vulnerability in Samsung Account prior to version 13.1.0.1 allows attackers to access to the authcode for sign-in.	6.2	More Details
CVE-2022-24399	The SAP Focused Run (Real User Monitoring) - versions 200, 300, REST service does not sufficiently sanitize the input name of the file using multipart/form-data, resulting in Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2022-24733	Sylius is an open source eCommerce platform. Prior to versions 1.9.10, 1.10.11, and 1.11.2, it is possible for a page controlled by an attacker to load the website within an iframe. This will enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. The issue is fixed in versions 1.9.10, 1.10.11, and 1.11.2. A workaround is available. Every response from app should have an X-Frame-Options header set to: ``sameorigin``. To achieve that, add a new `subscriber` in the app.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24749	Sylius is an open source eCommerce platform. In versions prior to 1.9.10, 1.10.11, and 1.11.2, it is possible to upload an SVG file containing cross-site scripting (XSS) code in the admin panel. In order to perform a XSS attack, the file itself has to be open in a new card or loaded outside of the IMG tag. The problem applies both to the files opened on the admin panel and shop pages. The issue is fixed in versions 1.9.10, 1.10.11, and 1.11.2. As a workaround, require a library that adds on-upload file sanitization and overwrite the service before writing the file to the filesystem. The GitHub Security Advisory contains more specific information about the workaround.	6.1	More Details
CVE-2021-46708	The swagger-ui-dist package before 4.1.3 for Node.js could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim.	6.1	More Details
CVE-2022-27193	CVRF-CSAF-Converter before 1.0.0-rc2 resolves XML External Entities (XXE). This leads to the inclusion of arbitrary (local) file content into the generated output document. An attacker can exploit this to disclose information from the system running the converter.	6.1	More Details
CVE-2022-0951	File Upload Restriction Bypass leading to Stored XSS Vulnerability in GitHub repository star7th/showdoc prior to 2.10.4.	6.1	More Details
CVE-2021-46709	phpLiteAdmin through 1.9.8.2 allows XSS via the index.php newRows parameter (aka num or number).	6.1	More Details
CVE-2021-41657	SmartBear CodeCollaborator v6.1.6102 was discovered to contain a vulnerability in the web UI which would allow an attacker to conduct a clickjacking attack.	6.1	More Details
CVE-2022-24608	Luocms v2.0 is affected by Cross Site Scripting (XSS) in /admin/news/sort_add.php and /inc/function.php.	6.1	More Details
CVE-2022-24397	SAP NetWeaver Enterprise Portal - versions 7.30, 7.31, 7.40, 7.50, does not sufficiently encode user-controlled inputs, resulting in reflected Cross-Site Scripting (XSS) vulnerability.This reflected cross-site scripting attack can be used to non-permanently deface or modify displayed content of portal Website. The execution of the script content by a victim registered on the portal could compromise the confidentiality and integrity of victim’s web browser.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26101	Fiori launchpad - versions 754, 755, 756, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2022-24395	SAP NetWeaver Enterprise Portal - versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not sufficiently encode user-controlled inputs, resulting in reflected Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2022-24177	A cross-site scripting (XSS) vulnerability in the component cgi-bin/ej.cgi of Ex libris ALEPH 500 v18.1 and v20 allows attackers to execute arbitrary web scripts or HTML.	6.1	More Details
CVE-2022-24746	Shopware is an open commerce platform based on the Symfony php Framework and the Vue javascript framework. In affected versions it is possible to inject code via the voucher code form. This issue has been patched in version 6.4.8.1. There are no known workarounds for this issue.	6.1	More Details
CVE-2022-0929	XSS on dynamic_text module in GitHub repository microweber/microweber prior to 1.2.11.	6.1	More Details
CVE-2022-26533	Alist v2.1.0 and below was discovered to contain a cross-site scripting (XSS) vulnerability via /i/:data/ipa.plist.	6.1	More Details
CVE-2022-0891	A heap buffer overflow in ExtractImageSection function in tiffcrop.c in libtiff library Version 4.3.0 allows attacker to trigger unsafe or out of bounds memory access via crafted TIFF image file which could result into application crash, potential information disclosure or any other context-dependent impact	6.1	More Details
CVE-2022-25493	HMS v1.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via treatmentrecord.php.	6.1	More Details
CVE-2022-24526	Visual Studio Code Spoofing Vulnerability	6.1	More Details
CVE-2022-25922	Power Line Communications PLC4TRUCKS J2497 trailer brake controllers implement diagnostic functions which can be invoked by replaying J2497 messages. There is no authentication or authorization for these functions.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0327	The Master Addons for Elementor WordPress plugin before 1.8.5 does not sanitise and escape the error_message parameter before outputting it back in the response of the jltma_restrict_content AJAX action, available to unauthenticated and authenticated users, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-32478	The redirect URI in the LTI authorization endpoint required extra sanitizing to prevent reflected XSS and open redirect risks. Moodle versions 3.10 to 3.10.3, 3.9 to 3.9.6, 3.8 to 3.8.8 and earlier unsupported versions are affected.	6.1	More Details
CVE-2021-25006	The MOLIE WordPress plugin through 0.5 does not escape the course_id parameter before outputting it back in the admin dashboard, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2022-0230	The Better WordPress Google XML Sitemaps WordPress plugin through 1.4.1 does not sanitise and escape its logs when outputting them in the admin dashboard, which could allow unauthenticated users to perform Stored Cross-Site Scripting attacks against admins	6.1	More Details
CVE-2022-0147	The Cookie Information | Free GDPR Consent Solution WordPress plugin before 2.0.8 does not escape user data before outputting it back in attributes in the admin dashboard, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2022-0820	Cross-site Scripting (XSS) - Stored in GitHub repository orchardcms/orchardcore prior to 1.3.0.	6.1	More Details
CVE-2022-0648	The Team Circle Image Slider With Lightbox WordPress plugin before 1.0.16 does not sanitize and escape the order_pos parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2021-24940	The Persian Woocommerce WordPress plugin through 5.8.0 does not escape the s parameter before outputting it back in an attribute in the admin dashboard, which could lead to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2022-0601	The Countdown, Coming Soon, Maintenance WordPress plugin before 2.2.9 does not sanitize and escape the post 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-2022-0503	The WordPress Multisite Content Copier/Updater WordPress plugin before 2.1.2 does not sanitise and escape the s parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting issue in the network dashboard	6.1	More Details
CVE-2022-0449	The Flexi WordPress plugin before 4.20 does not sanitise and escape various parameters before outputting them back in some pages such as the user dashboard, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-0165	The Page Builder KingComposer WordPress plugin through 2.9.6 does not validate the id parameter before redirecting the user to it via the kc_get_thumbn AJAX action available to both unauthenticated and authenticated users	6.1	More Details
CVE-2022-0161	The ARI Fancy Lightbox WordPress plugin before 1.3.9 does not sanitise and escape the msg parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-24996	The IDPay for Contact Form 7 WordPress plugin through 2.1.2 does not sanitise and escape the idpay_error parameter before outputting it back in the page leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-22734	The Simple Quotation WordPress plugin through 1.3.2 does not have CSRF check when creating or editing a quote and does not sanitise and escape Quotes. As a result, attacker could make a logged in admin create or edit arbitrary quote, and put Cross-Site Scripting payloads in them	6.1	More Details
CVE-2022-0399	The Advanced Product Labels for WooCommerce WordPress plugin before 1.2.3.7 does not sanitise and escape the tax_color_set_type parameter before outputting it back in the berocket_apl_color_listener AJAX action's response, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-44585	A Cross Site Scripting (XSS) vulnerabilitiy exits in jeecg-boot 3.0 in /jeecg-boot/jmreport/view with a mouseover event.	6.1	More Details
CVE-2022-22344	IBM Spectrum Copy Data Management 2.2.0.0 through 2.2.14.3 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 220038	6.1	More Details
CVE-2021-44667	A Cross Site Scripting (XSS) vulnerability exists in Nacos 2.0.3 in auth/users via the (1) pageSize and (2) pageNo parameters.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0248	The Contact Form Submissions WordPress plugin before 1.7.3 does not sanitise and escape additional fields in contact form requests before outputting them in the related submission. As a result, unauthenticated attacker could perform Cross-Site Scripting attacks against admins viewing the malicious submission	6.1	More Details
CVE-2022-0321	The WP Voting Contest WordPress plugin before 3.0 does not sanitise and escape the post_id parameter before outputting it back in the response via the wpvc_social_share_icons AJAX action (available to both unauthenticated and authenticated users), leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-40055	There is a man-in-the-middle attack vulnerability during system update download in recovery mode. Successful exploitation of this vulnerability may affect integrity.	5.9	More Details
CVE-2022-23278	Microsoft Defender for Endpoint Spoofing Vulnerability	5.9	More Details
CVE-2022-24928	Security misconfiguration of RKP in kernel prior to SMR Mar-2022 Release 1 allows a system not to be protected by RKP.	5.9	More Details
CVE-2022-0507	Found a potential security vulnerability inside the Pandora API. Affected Pandora FMS version range: all versions of NG version, up to OUM 759. This vulnerability could allow an attacker with authenticated IP to inject SQL.	5.8	More Details
CVE-2022-23960	Certain Arm Cortex and Neoverse processors through 2022-03-08 do not properly restrict cache speculation, aka Spectre-BHB. An attacker can leverage the shared branch history in the Branch History Buffer (BHB) to influence mispredicted branches. Then, cache allocation can allow the attacker to obtain sensitive information.	5.6	More Details
CVE-2021-26401	LFENCE/JMP (mitigation V2-2) may not sufficiently mitigate CVE-2017-5715 on some AMD CPUs.	5.6	More Details
CVE-2021-41849	An issue was discovered in Luna Simo PPR1.180610.011/202001031830. It sends the following Personally Identifiable Information (PII) in plaintext using HTTP to servers located in China: user's list of installed apps and device International Mobile Equipment Identity (IMEI). This PII is transmitted to log.skyroam.com.cn using HTTP, independent of whether the user uses the Simo software.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21973	Windows Media Center Update Denial of Service Vulnerability	5.5	More Details
CVE-2022-24576	GPAC 1.0.1 is affected by Use After Free through MP4Box.	5.5	More Details
CVE-2022-26966	An issue was discovered in the Linux kernel before 5.16.12. drivers/net/usb/sr9700.c allows attackers to obtain sensitive information from heap memory via crafted frame lengths from a device.	5.5	More Details
CVE-2022-23281	Windows Common Log File System Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2022-0968	The microweber application allows large characters to insert in the input field "fist & last name" which can allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request. in microweber/microweber in GitHub repository microweber/microweber prior to 1.2.12.	5.5	More Details
CVE-2022-0961	The microweber application allows large characters to insert in the input field "post title" which can allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request. in GitHub repository microweber/microweber prior to 1.2.12.	5.5	More Details
CVE-2021-25026	The Patreon WordPress plugin before 1.8.2 does not sanitise and escape the field "Custom Patreon Page name", which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	5.5	More Details
CVE-2022-23297	Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2022-24511	Microsoft Office Word Tampering Vulnerability	5.5	More Details
CVE-2022-24462	Microsoft Word Security Feature Bypass Vulnerability	5.5	More Details
CVE-2022-24574	GPAC 1.0.1 is affected by a NULL pointer dereference in gf_dump_vrml_field.isra ().	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27195	Jenkins Parameterized Trigger Plugin 2.43 and earlier captures environment variables passed to builds triggered using Jenkins Parameterized Trigger Plugin, including password parameter values, in their `build.xml` files. These values are stored unencrypted and can be viewed by users with access to the Jenkins controller file system.	5.5	More Details
CVE-2022-20051	In ims service, there is a possible unexpected application behavior due to incorrect privilege assignment. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219127; Issue ID: ALPS06219127.	5.5	More Details
CVE-2021-27414	An attacker could trick a user of Hitachi ABB Power Grids Ellipse Enterprise Asset Management (EAM) versions prior to and including 9.0.25 into visiting a malicious website posing as a login page for the Ellipse application and gather authentication credentials.	5.5	More Details
CVE-2022-26878	drivers/bluetooth/virtio_bt.c in the Linux kernel before 5.16.3 has a memory leak (socket buffers have memory allocated but not freed).	5.5	More Details
CVE-2022-0907	Unchecked Return Value to NULL Pointer Dereference 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 f2b656e2.	5.5	More Details
CVE-2022-0909	Divide By Zero 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 f8d0f9aa.	5.5	More Details
CVE-2022-0924	Out-of-bounds Read error in tiffcp 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 408976c4.	5.5	More Details
CVE-2021-20269	A flaw was found in the permissions of a log file created by kexec-tools. This flaw allows a local unprivileged user to read this file and leak kernel internal information from a previous panic. The highest threat from this vulnerability is to confidentiality. This flaw affects kexec-tools shipped by Fedora versions prior to 2.0.21-8 and RHEL versions prior to 2.0.20-47.	5.5	More Details
CVE-2021-4023	A flaw was found in the io-workqueue implementation in the Linux kernel versions prior to 5.15-rc1. The kernel can panic when an improper cancellation operation triggers the submission of new io-uring operations during a shortage of free space. This flaw allows a local user with permissions to execute io-uring requests to possibly crash the system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24432	Persistent cross-site scripting (XSS) in the web interface of ipDIO allows an authenticated remote attacker to introduce arbitrary JavaScript by injecting an XSS payload into specific fields. The XSS payload will be executed when a legitimate user attempts to upload, copy, download, or delete an existing configuration (Administrative Services).	5.5	More Details
CVE-2021-3732	A flaw was found in the Linux kernel's OverlayFS subsystem in the way the user mounts the TmpFS filesystem with OverlayFS. This flaw allows a local user to gain access to hidden files that should not be accessible.	5.5	More Details
CVE-2021-44215	Northern.tech CFEngine Enterprise 3.15.4 before 3.15.5 has Insecure Permissions that may allow unauthorized local users to have an unspecified impact.	5.5	More Details
CVE-2022-0890	NULL Pointer Dereference in GitHub repository mruby/mruby prior to 3.2.	5.5	More Details
CVE-2022-25815	PendingIntent hijacking vulnerability in Weather application prior to SMR Mar-2022 Release 1 allows local attackers to perform unauthorized action without permission via hijacking the PendingIntent.	5.5	More Details
CVE-2021-32434	abcm2ps v8.14.11 was discovered to contain an out-of-bounds read in the function calculate_beam at draw.c.	5.5	More Details
CVE-2022-25814	PendingIntent hijacking vulnerability in Wearable Manager Installer prior to SMR Mar-2022 Release 1 allows local attackers to perform unauthorized action without permission via hijacking the PendingIntent.	5.5	More Details
CVE-2021-34122	The function bitstr_tell at bitstr.c in ffjpeg commit 4ab404e has a NULL pointer dereference.	5.5	More Details
CVE-2022-0865	Reachable Assertion in tiffcp 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 5e180045.	5.5	More Details
CVE-2022-24090	Adobe Photoshop versions 23.1.1 (and earlier) and 22.5.5 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0433	A NULL pointer dereference flaw was found in the Linux kernel's BPF subsystem in the way a user triggers the map_get_next_key function of the BPF bloom filter. This flaw allows a local user to crash the system. This flaw affects Linux kernel versions prior to 5.17-rc1.	5.5	More Details
CVE-2021-4095	A NULL pointer dereference was found in the Linux kernel's KVM when dirty ring logging is enabled without an active vCPU context. An unprivileged local attacker on the host may use this flaw to cause a kernel oops condition and thus a denial of service by issuing a KVM_XEN_HVM_SET_ATTR ioctl. This flaw affects Linux kernel versions prior to 5.17-rc1.	5.5	More Details
CVE-2022-25108	Foxit PDF Reader and Editor before 11.2.1 and PhantomPDF before 10.1.7 allow a NULL pointer dereference during PDF parsing because the pointer is used without proper validation.	5.5	More Details
CVE-2021-27416	An attacker could exploit this vulnerability in Hitachi ABB Power Grids Ellipse Enterprise Asset Management (EAM) versions prior to and including 9.0.25 by tricking a user to click on a link containing malicious code that would then be run by the web browser. This can result in the compromise of confidential information, or even the takeover of the user’s session.	5.5	More Details
CVE-2021-32435	Stack-based buffer overflow in the function get_key in parse.c of abcm2ps v8.14.11 allows remote attackers to cause a Denial of Service (DoS) via unspecified vectors.	5.5	More Details
CVE-2021-44421	The pointer-validation logic in util/mem_util.rs in Occlum before 0.26.0 for Intel SGX acts as a confused deputy that allows a local attacker to access unauthorized information via side-channel analysis.	5.5	More Details
CVE-2021-44269	An out of bounds read was found in Wavpack 5.4.0 in processing *.WAV files. This issue triggered in function WavpackPackSamples of file src/pack_utils.c, tainted variable cnt is too large, that makes pointer sptr read beyond heap bound.	5.5	More Details
CVE-2021-44216	Northern.tech CFEngine Enterprise before 3.15.5 and 3.18.x before 3.18.1 has Insecure Permissions that may allow unauthorized local users to access the Apache and Mission Portal log files.	5.5	More Details
CVE-2022-0942	Stored XSS due to Unrestricted File Upload in GitHub repository star7th/showdoc prior to 2.10.4.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0928	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.2.12.	5.4	More Details
CVE-2021-33851	A cross-site scripting (XSS) attack can cause arbitrary code (JavaScript) to run in a user's browser and can use an application as the vehicle for the attack. The XSS payload given in the "Custom logo link" executes whenever the user opens the Settings Page of the "Customize Login Image" Plugin.	5.4	More Details
CVE-2021-33852	A cross-site scripting (XSS) attack can cause arbitrary code (JavaScript) to run in a user's browser and can use an application as the vehicle for the attack. The XSS payload given in the "Duplicate Title" text box executes whenever the user opens the Settings Page of the Post Duplicator Plugin or the application root page after duplicating any of the existing posts.	5.4	More Details
CVE-2022-24503	Remote Desktop Protocol Client Information Disclosure Vulnerability	5.4	More Details
CVE-2022-0954	Multiple Stored Cross-site Scripting (XSS) Vulnerabilities in Shop's Other Settings, Shop's Autorespond E-mail Settings and Shops' Payments Methods in GitHub repository microweber/microweber prior to 1.2.11.	5.4	More Details
CVE-2022-0894	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.4.0.	5.4	More Details
CVE-2022-26874	lib/Horde/Mime/Viewer/Ooo.php in Horde Mime_Viewer before 2.2.4 allows XSS via an OpenOffice document, leading to account takeover in Horde Groupware Webmail Edition. This occurs after XSLT rendering.	5.4	More Details
CVE-2022-27202	Jenkins Extended Choice Parameter Plugin 346.vd87693c5a_86c and earlier does not escape the value and description of extended choice parameters of radio buttons or check boxes type, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-0822	Cross-site Scripting (XSS) - Reflected in GitHub repository orchardcms/orchardcore prior to 1.3.0.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24958	The Meks Easy Photo Feed Widget WordPress plugin before 1.2.4 does not have capability and CSRF checks in the meks_save_business_selected_account AJAX action, available to any authenticated user, and does not escape some of the settings. As a result, any authenticated user, such as subscriber could update the plugin's settings and put Cross-Site Scripting payloads in them	5.4	More Details
CVE-2022-27196	Jenkins Favorite Plugin 2.4.0 and earlier does not escape the names of jobs in the favorite column, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure or Item/Create permissions.	5.4	More Details
CVE-2022-25507	FreeTAKServer-UI v1.9.8 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Callsign parameter.	5.4	More Details
CVE-2022-0963	Unrestricted XML Files Leads to Stored XSS in GitHub repository microweber/microweber prior to 1.2.12.	5.4	More Details
CVE-2022-0964	Stored XSS viva .webmv file upload in GitHub repository star7th/showdoc prior to 2.10.4.	5.4	More Details
CVE-2022-0965	Stored XSS viva .ofd file upload in GitHub repository star7th/showdoc prior to 2.10.4.	5.4	More Details
CVE-2022-0966	Stored XSS via File Upload in star7th/showdoc in GitHub repository star7th/showdoc prior to 2.4.10.	5.4	More Details
CVE-2022-26102	Due to missing authorization check, SAP NetWeaver Application Server for ABAP - versions 700, 701, 702, 731, allows an authenticated attacker, to access content on the start screen of any transaction that is available with in the same SAP system even if he/she isn't authorized for that transaction. A successful exploitation could expose information and in worst case manipulate data before the start screen is executed, resulting in limited impact on confidentiality and integrity of the application.	5.4	More Details
CVE-2022-0960	Stored XSS viva .properties file upload in GitHub repository star7th/showdoc prior to 2.10.4.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0962	Stored XSS viva .webma file upload in GitHub repository star7th/showdoc prior to 2.10.4.	5.4	More Details
CVE-2022-0970	Cross-site Scripting (XSS) - Stored in GitHub repository getgrav/grav prior to 1.7.31.	5.4	More Details
CVE-2021-39055	IBM Spectrum Copy Data Management 2.2.0.0 through 2.2.14.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 214534.	5.4	More Details
CVE-2022-27197	Jenkins Dashboard View Plugin 2.18 and earlier does not perform URL validation for the Iframe Portlet's Iframe source URL, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to configure views.	5.4	More Details
CVE-2021-24950	The Insight Core WordPress plugin through 1.0 does not have any authorisation and CSRF checks in the insight_customizer_options_import (available to any authenticated user), does not validate user input before passing it to unserialize(), nor sanitise and escape it before outputting it in the response. As a result, it could allow users with a role as low as Subscriber to perform PHP Object Injection, as well as Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-0967	Stored XSS via File Upload in star7th/showdoc in star7th/showdoc in GitHub repository star7th/showdoc prior to 2.10.4.	5.4	More Details
CVE-2022-0938	Stored XSS via file upload in GitHub repository star7th/showdoc prior to v2.10.4.	5.4	More Details
CVE-2022-0880	Cross-site Scripting (XSS) - Stored in GitHub repository star7th/showdoc prior to 2.10.2.	5.4	More Details
CVE-2022-0950	Unrestricted Upload of File with Dangerous Type in GitHub repository star7th/showdoc prior to 2.10.4.	5.4	More Details
CVE-2022-0945	Stored XSS viva axd and cshtml file upload in star7th/showdoc in GitHub repository star7th/showdoc prior to v2.10.4.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27213	Jenkins Environment Dashboard Plugin 1.1.10 and earlier does not escape the Environment order and the Component order configuration values in its views, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with View/Configure permission.	5.4	More Details
CVE-2021-24897	The Add Subtitle WordPress plugin through 1.1.0 does not sanitise or escape the sub-title field (available only with classic editor) when output in the page, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks	5.4	More Details
CVE-2022-27212	Jenkins List Git Branches Parameter Plugin 0.0.9 and earlier does not escape the name of the 'List Git branches (and more)' parameter, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-0956	Stored XSS via File Upload in GitHub repository star7th/showdoc prior to v.2.10.4.	5.4	More Details
CVE-2022-25489	Atom CMS v2.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the "A" parameter in /widgets/debug.php.	5.4	More Details
CVE-2021-45889	An issue was discovered in PONTON X/P Messenger before 3.11.2. Several functions are vulnerable to reflected XSS, as demonstrated by private/index.jsp?partners/ShowNonLocalPartners.do?localID= or private/index.jsp or private/index.jsp?database/databaseTab.jsp or private/index.jsp?activation/activationMainTab.jsp or private/index.jsp?communication/serverTab.jsp or private/index.jsp?emailNotification/notificationTab.jsp.	5.4	More Details
CVE-2022-22511	Various configuration pages of the device are vulnerable to reflected XSS (Cross-Site Scripting) attacks. An authorized attacker with user privileges may use this to gain access to confidential information on a PC that connects to the WBM after it has been compromised.	5.4	More Details
CVE-2022-0937	Stored xss in showdoc through file upload in GitHub repository star7th/showdoc prior to 2.10.4.	5.4	More Details
CVE-2022-0341	Cross-site Scripting (XSS) - Stored in GitHub repository vanessa219/vditor prior to 3.8.12.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0940	Stored XSS due to Unrestricted File Upload in GitHub repository star7th/showdoc prior to v2.10.4.	5.4	More Details
CVE-2022-0946	Stored XSS viva cshtm file upload in GitHub repository star7th/showdoc prior to v2.10.4.	5.4	More Details
CVE-2022-0957	Stored XSS via File Upload in GitHub repository star7th/showdoc prior to 2.10.4.	5.4	More Details
CVE-2022-21158	A stored cross-site scripting vulnerability in marktext versions prior to v0.17.0 due to improper handling of the link (with javascript: scheme) inside the document may allow an attacker to execute an arbitrary script on the PC of the user using marktext.	5.4	More Details
CVE-2022-25600	Cross-Site Request Forgery (CSRF) vulnerability affecting Delete Marker Category, Delete Map, and Copy Map functions in WP Google Map plugin (versions <= 4.2.3).	5.4	More Details
CVE-2022-0893	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.4.0.	5.4	More Details
CVE-2021-32475	ID numbers displayed in the quiz grading report required additional sanitizing to prevent a stored XSS risk. Moodle 3.10 to 3.10.3, 3.9 to 3.9.6, 3.8 to 3.8.8, 3.5 to 3.5.17 and earlier unsupported versions are affected.	5.4	More Details
CVE-2022-0941	Stored XSS due to Unrestricted File Upload in GitHub repository star7th/showdoc prior to v2.10.4.	5.4	More Details
CVE-2022-26847	SPIP before 3.2.14 and 4.x before 4.0.5 allows unauthenticated access to information about editorial objects.	5.3	More Details
CVE-2022-25215	Improper access control on the LocalMACConfig.asp interface allows an unauthenticated remote attacker to add (or remove) client MAC addresses to (or from) a list of banned hosts. Clients with those MAC addresses are then prevented from accessing either the WAN or the router itself.	5.3	More Details
CVE-2022-0903	A call stack overflow bug in the SAML login feature in Mattermost server in versions up to and including 6.3.2 allows an attacker to crash the server via submitting a maliciously crafted POST body.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26104	SAP Financial Consolidation - version 10.1, does not perform necessary authorization checks for updating homepage messages, resulting for an unauthorized user to alter the maintenance system message.	5.3	More Details
CVE-2022-25497	CuppaCMS v1.0 was discovered to contain an arbitrary file read via the copy function.	5.3	More Details
CVE-2021-29134	The avatar middleware in Gitea before 1.13.6 allows Directory Traversal via a crafted URL.	5.3	More Details
CVE-2021-38910	IBM DataPower Gateway V10CD, 10.0.1, and 2108.4.1 could allow a remote attacker to bypass security restrictions, caused by the improper validation of input. By sending a specially crafted JSON message, an attacker could exploit this vulnerability to modify structure and fields. IBM X-Force ID: 209824.	5.3	More Details
CVE-2021-39025	IBM Guardium Data Encryption (GDE) 4.0.0.0 and 5.0.0.0 could disclose internal IP address information when the web backend is down. IBM X-Force 213863.	5.3	More Details
CVE-2022-26778	Veritas System Recovery (VSR) 18 and 21 stores a network destination password in the Windows registry during configuration of the backup configuration. This could allow a Windows user (who has sufficient privileges) to access a network file system that they were not authorized to access.	5.3	More Details
CVE-2022-26103	Under certain conditions, SAP NetWeaver (Real Time Messaging Framework) - version 7.50, allows an attacker to access information which could lead to information gathering for further exploits and attacks.	5.3	More Details
CVE-2022-24322	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause a disruption of communication between the Modicon controller and the engineering software when an attacker is able to intercept and manipulate specific Modbus response data. Affected Product: EcoStruxure Control Expert (V15.0 SP1 and prior)	5.3	More Details
CVE-2022-24323	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause a disruption of communication between the Modicon controller and the engineering software, when an attacker is able to intercept and manipulate specific Modbus response data. Affected Product: EcoStruxure Process Expert (V2021 and prior), EcoStruxure Control Expert (V15.0 SP1 and prior)	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26276	An issue in index.php of OneNav v0.9.14 allows attackers to perform directory traversal.	5.3	More Details
CVE-2021-42857	It was discovered that the SteelCentral AppInternals Dynamic Sampling Agent's (DSA) AgentDaServlet has directory traversal vulnerabilities at the "/api/appInternals/1.0/agent/da/pcf" API. The affected endpoint does not have any validation of the user's input that allows a malicious payload to be injected.	5.3	More Details
CVE-2021-35251	Sensitive information could be displayed when a detailed technical error message is posted. This information could disclose environmental details about the Web Help Desk installation.	5.3	More Details
CVE-2022-0813	PhpMyAdmin 5.1.1 and before allows an attacker to retrieve potentially sensitive information by creating invalid requests. This affects the lang parameter, the pma_parameter, and the cookie section.	5.3	More Details
CVE-2022-0430	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository httpie/httpie prior to 3.1.0.	5.3	More Details
CVE-2022-0870	Server-Side Request Forgery (SSRF) in GitHub repository gogs/gogs prior to 0.12.5.	5.3	More Details
CVE-2021-32473	It was possible for a student to view their quiz grade before it had been released, using a quiz web service. Moodle 3.10 to 3.10.3, 3.9 to 3.9.6, 3.8 to 3.8.8, 3.5 to 3.5.17 and earlier unsupported versions are affected	5.3	More Details
CVE-2022-25819	OOB read vulnerability in hdcp2 device node prior to SMR Mar-2022 Release 1 allow an attacker to view Kernel stack memory.	5.3	More Details
CVE-2020-14112	Information Leak Vulnerability exists in the Xiaomi Router AX6000. The vulnerability is caused by incorrect routing configuration. Attackers can exploit this vulnerability to download part of the files in Xiaomi Router AX6000.	5.3	More Details
CVE-2022-24742	Sylius is an open source eCommerce platform. Prior to versions 1.9.10, 1.10.11, and 1.11.2, any other user can view the data if browser tab remains unclosed after log out. The issue is fixed in versions 1.9.10, 1.10.11, and 1.11.2. A workaround is available. The application must strictly redirect to login page even browser back button is pressed. Another possibility is to set more strict cache policies for restricted content.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32006	This issue affects: Secomea GateManager Version 9.6.621421014 and all prior versions. Permission Issues vulnerability in LinkManager web portal of Secomea GateManager allows logged in LinkManager user to access stored SiteManager backup files.	5.0	More Details
CVE-2021-32009	Cross-site Scripting (XSS) vulnerability in firmware section of Secomea GateManager allows logged in user to inject javascript in browser session. This issue affects: Secomea GateManager Version 9.6.621421014 and all prior versions.	5.0	More Details
CVE-2022-24740	Volto is a ReactJS-based frontend for the Plone Content Management System. Between versions 14.0.0-alpha.5 and 15.0.0-alpha.0, a user could have their authentication cookie replaced with an authentication cookie from another user, effectively giving them control of the other user's account and privileges. This occurs when using an outdated version of the `react-cookie` library and a server is under high load. A proof of concept does not currently exist, but it is possible for this issue to occur in the wild. The patch and fix is present in Volto 15.0.0-alpha.0. As a workaround, one may manually upgrade the `react-cookie` package to 4.1.1 and then override all Volto components that use this library.	5.0	More Details
CVE-2021-38971	IBM Data Virtualization on Cloud Pak for Data 1.3.0, 1.4.1, 1.5.0, 1.7.1 and 1.7.3 could allow an authorized user to bypass data masking rules and obtain sensitve information. IBM X-Force ID: 212620.	4.9	More Details
CVE-2021-24966	The Error Log Viewer WordPress plugin through 1.1.1 does not validate the path of the log file to clear, allowing high privilege users to clear arbitrary files on the web server, including those outside of the blog folder	4.9	More Details
CVE-2022-0703	The GD Mylist WordPress plugin through 1.1.1 does not sanitise and escape some of its settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-0702	The Petfinder Listings WordPress plugin through 1.0.18 does not escape its settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-0926	File upload filter bypass leading to stored XSS in GitHub repository microweber/microweber prior to 1.2.12.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24745	Shopware is an open commerce platform based on the Symfony php Framework and the Vue javascript framework. In affected versions guest sessions are shared between customers when HTTP cache is enabled. This can lead to inconsistent experiences for guest users. Setups with Varnish are not affected by this issue. This issue has been resolved in version 6.4.8.2. Users unable to upgrade should disable the HTTP Cache.	4.8	More Details
CVE-2022-0930	File upload filter bypass leading to stored XSS in GitHub repository microweber/microweber prior to 1.2.12.	4.8	More Details
CVE-2022-0906	Unrestricted file upload leads to stored XSS in GitHub repository microweber/microweber prior to 1.1.12.	4.8	More Details
CVE-2021-45888	An issue was discovered in PONTON X/P Messenger before 3.11.2. The navigation tree that is shown on the left side of every page of the web application is vulnerable to XSS: it allows injection of JavaScript into its nodes. Creating such nodes is only possible for users who have the role Configuration Administrator or Administrator.	4.8	More Details
CVE-2021-24895	The Cybersoldier WordPress plugin before 1.7.0 does not sanitise and escape the URL settings before outputting it in an attribute, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2021-24995	The HTML5 Responsive FAQ WordPress plugin through 2.8.5 does not properly sanitise and escape some of its settings, which could allow a high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed	4.8	More Details
CVE-2021-41952	Zenario CMS 9.0.54156 is vulnerable to Cross Site Scripting (XSS) via upload file to *.SVG. An attacker can send malicious files to victims and steals victim's cookie leads to account takeover. The person viewing the image of a contact can be victim of XSS.	4.8	More Details
CVE-2022-27207	Jenkins global-build-stats Plugin 1.5 and earlier does not escape multiple fields in the chart configuration on the 'Global Build Stats' page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Overall/Administer permission.	4.8	More Details
CVE-2022-27200	Jenkins Folder-based Authorization Strategy Plugin 1.3 and earlier does not escape the names of roles shown on the configuration form, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Overall/Administer permission.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0659	The Sync QCloud COS WordPress plugin before 2.0.1 does not escape some of its settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-0674	The Kunze Law WordPress plugin before 2.1 does not escape its 'E-Mail Error "From" Address' settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-0684	The WP Home Page Menu WordPress plugin before 3.1 does not sanitise and escape its settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-0700	The Simple Tracking WordPress plugin before 1.7 does not sanitise and escape its settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-0701	The SEO 301 Meta WordPress plugin through 1.9.1 does not escape its Request and Destination settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2022-0912	Unrestricted Upload of File with Dangerous Type in GitHub repository microweber/microweber prior to 1.2.11.	4.8	More Details
CVE-2021-42856	It was discovered that the /DsaDataTest endpoint is susceptible to Cross-site scripting (XSS) attack. It was noted that the Metric parameter does not have any input checks on the user input that allows an attacker to craft its own malicious payload to trigger a XSS vulnerability.	4.7	More Details
CVE-2022-25368	Spectre BHB is a variant of Spectre-v2 in which malicious code uses the shared branch history (stored in the CPU BHB) to influence mispredicted branches in the victim's hardware context. Speculation caused by these mispredicted branches can then potentially be used to cause cache allocation, which can then be used to infer information that should be protected.	4.7	More Details
CVE-2022-21975	Windows Hyper-V Denial of Service Vulnerability	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25601	Reflected Cross-Site Scripting (XSS) vulnerability affecting parameter &tab discovered in Contact Form X WordPress plugin (versions <= 2.4).	4.7	More Details
CVE-2022-24349	An authenticated user can create a link with reflected XSS payload for actions' pages, and send it to other users. Malicious code has access to all the same objects as the rest of the web page and can make arbitrary modifications to the contents of the page being displayed to a victim. This attack can be implemented with the help of social engineering and expiration of a number of factors - an attacker should have authorized access to the Zabbix Frontend and allowed network connection between a malicious server and victim's computer, understand attacked infrastructure, be recognized by the victim as a trustee and use trusted communication channel.	4.6	More Details
CVE-2022-24930	An Improper access control vulnerability in StRetailModeReceiver in Wear OS 3.0 prior to Firmware update MAR-2022 Release allows untrusted applications to reset default app settings without a proper permission	4.4	More Details
CVE-2022-22010	Media Foundation Information Disclosure Vulnerability	4.4	More Details
CVE-2022-26355	Citrix Federated Authentication Service (FAS) 7.17 - 10.6 causes deployments that have been configured to store a registration authority certificate's private key in a Trusted Platform Module (TPM) to incorrectly store that key in the Microsoft Software Key Storage Provider (MSKSP). This issue only occurs if PowerShell was used when configuring FAS to store the registration authority certificate's private key in the TPM. It does not occur if the TPM was not selected for use or if the FAS administration console was used for configuration.	4.4	More Details
CVE-2022-27215	A missing permission check in Jenkins Release Helper Plugin 1.3.3 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials.	4.3	More Details
CVE-2022-27218	Jenkins incapptic connect uploader Plugin 1.15 and earlier stores tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Extended Read permission, or access to the Jenkins controller file system.	4.3	More Details
CVE-2021-43954	The DefaultRepositoryAdminService class in Fisheye and Crucible before version 4.8.9 allowed remote attackers, who have 'can add repository permission', to enumerate the existence of internal network and filesystem resources via a Server-Side Request Forgery (SSRF) vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27205	A missing permission check in Jenkins Extended Choice Parameter Plugin 346.vd87693c5a_86c and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL.	4.3	More Details
CVE-2018-25031	Swagger UI 4.1.2 and earlier could allow a remote attacker to conduct spoofing attacks. By persuading a victim to open a crafted URL, an attacker could exploit this vulnerability to display remote OpenAPI definitions. Note: This was originally claimed to be resolved in 4.1.3. However, third parties have indicated this is not resolved in 4.1.3 and even occurs in that version and possibly others.	4.3	More Details
CVE-2022-24502	Windows HTML Platforms Security Feature Bypass Vulnerability	4.3	More Details
CVE-2022-27199	A missing permission check in Jenkins CloudBees AWS Credentials Plugin 189.v3551d5642995 and earlier allows attackers with Overall/Read permission to connect to an AWS service using an attacker-specified token.	4.3	More Details
CVE-2021-3660	Cockpit (and its plugins) do not seem to protect itself against clickjacking. It is possible to render a page from a cockpit server via another website, inside an <iFrame> HTML entry. This may be used by a malicious website in clickjacking or similar attacks.	4.3	More Details
CVE-2022-27214	A cross-site request forgery (CSRF) vulnerability in Jenkins Release Helper Plugin 1.3.3 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials.	4.3	More Details
CVE-2021-32472	Teachers exporting a forum in CSV format could receive a CSV of forums from all courses in some circumstances. Moodle versions 3.10 to 3.10.3, 3.9 to 3.9.6 and 3.8 to 3.8.8 are affected.	4.3	More Details
CVE-2020-4989	IBM Engineering Workflow Management 7.0, 7.0.1, and 7.0.2 and IBM Rational Team Concert 6.0.6 and 6.0.0.1 could allow an authenticated user to obtain sensitive information about build definitions. IBM X-Force ID: 192707.	4.3	More Details
CVE-2021-32477	The last time a user accessed the mobile app is displayed on their profile page, but should be restricted to users with the relevant capability (site administrators by default). Moodle versions 3.10 to 3.10.3 are affected.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25839	The package url-js before 2.1.0 are vulnerable to Improper Input Validation due to improper parsing, which makes it is possible for the hostname to be spoofed. http://\\\\\\\\localhost and http://localhost are the same URL. However, the hostname is not parsed as localhost, and the backslash is reflected as it is.	4.3	More Details
CVE-2022-0904	A stack overflow bug in the document extractor in Mattermost Server in versions up to and including 6.3.2 allows an attacker to crash the server via submitting a maliciously crafted Apple Pages document.	4.3	More Details
CVE-2022-25820	A vulnerable design in fingerprint matching algorithm prior to SMR Mar-2022 Release 1 allows physical attackers to perform brute force attack on screen lock password.	4.2	More Details
CVE-2022-24932	Improper Protection of Alternate Path vulnerability in Setup wizard process prior to SMR Mar-2022 Release 1 allows physical attacker package installation before finishing Setup wizard.	4.2	More Details
CVE-2022-24929	Unprotected Activity in AppLock prior to SMR Mar-2022 Release 1 allows attacker to change the list of locked app without authentication.	4.1	More Details
CVE-2022-0022	Usage of a weak cryptographic algorithm in Palo Alto Networks PAN-OS software where the password hashes of administrator and local user accounts are not created with a sufficient level of computational effort, which allows for password cracking attacks on accounts in normal (non-FIPS-CC) operational mode. An attacker must have access to the account password hashes to take advantage of this weakness and can acquire those hashes if they are able to gain access to the PAN-OS software configuration. Fixed versions of PAN-OS software use a secure cryptographic algorithm for account password hashes. This issue does not impact Prisma Access firewalls. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.21; All versions of PAN-OS 9.0; PAN-OS 9.1 versions earlier than PAN-OS 9.1.11; PAN-OS 10.0 versions earlier than PAN-OS 10.0.7.	4.1	More Details
CVE-2022-25816	Improper authentication in Samsung Lock and mask apps setting prior to SMR Mar-2022 Release 1 allows attacker to change enable/disable without authentication	4.1	More Details
CVE-2022-25824	Improper access control vulnerability in BixbyTouch prior to version 2.2.00.6 in China models allows untrusted applications to load arbitrary URL and local files in webview.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25822	An use after free vulnerability in sdp driver prior to SMR Mar-2022 Release 1 allows kernel crash.	4.0	More Details
CVE-2022-25817	Improper authentication in One UI Home prior to SMR Mar-2022 Release 1 allows attacker to generate pinned-shortcut without user consent.	4.0	More Details
CVE-2022-24917	An authenticated user can create a link with reflected Javascript code inside it for services' page and send it to other users. The payload can be executed only with a known CSRF token value of the victim, which is changed periodically and is difficult to predict. Malicious code has access to all the same objects as the rest of the web page and can make arbitrary modifications to the contents of the page being displayed to a victim during social engineering attacks.	3.7	More Details
CVE-2022-21170	Improper check for certificate revocation in i-FILTER Ver.10.45R01 and earlier, i-FILTER Ver.9.50R10 and earlier, i-FILTER Browser & Cloud MultiAgent for Windows Ver.4.93R04 and earlier, and D-SPA (Ver.3 / Ver.4) using i-FILTER allows a remote unauthenticated attacker to conduct a man-in-the-middle attack and eavesdrop on an encrypted communication.	3.7	More Details
CVE-2021-36368	An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed.	3.7	More Details
CVE-2022-24918	An authenticated user can create a link with reflected Javascript code inside it for items' page and send it to other users. The payload can be executed only with a known CSRF token value of the victim, which is changed periodically and is difficult to predict. Malicious code has access to all the same objects as the rest of the web page and can make arbitrary modifications to the contents of the page being displayed to a victim during social engineering attacks.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24919	An authenticated user can create a link with reflected Javascript code inside it for graphs' page and send it to other users. The payload can be executed only with a known CSRF token value of the victim, which is changed periodically and is difficult to predict. Malicious code has access to all the same objects as the rest of the web page and can make arbitrary modifications to the contents of the page being displayed to a victim during social engineering attacks.	3.7	More Details
CVE-2022-24741	Nextcloud server is an open source, self hosted cloud style services platform. In affected versions an attacker can cause a denial of service by uploading specially crafted files which will cause the server to allocate too much memory / CPU. It is recommended that the Nextcloud Server is upgraded to 21.0.8 , 22.2.4 or 23.0.1. Users unable to upgrade should disable preview generation with the `'enable_previews'` config flag.	3.5	More Details
CVE-2022-21977	Media Foundation Information Disclosure Vulnerability	3.3	More Details
CVE-2022-25821	Improper use of SMS buffer pointer in Shannon baseband prior to SMR Mar-2022 Release 1 allows OOB read.	3.3	More Details
CVE-2021-3981	A flaw in grub2 was found where its configuration file, known as grub.cfg, is being created with the wrong permission set allowing non privileged users to read its content. This represents a low severity confidentiality issue, as those users can eventually read any encrypted passwords present in grub.cfg. This flaw affects grub2 2.06 and previous versions. This issue has been fixed in grub upstream but no version with the fix is currently released.	3.3	More Details
CVE-2022-24465	Microsoft Intune Portal for iOS Security Feature Bypass Vulnerability	3.3	More Details
CVE-2022-24744	Shopware is an open commerce platform based on the Symfony php Framework and the Vue javascript framework. In affected versions user sessions are not logged out if the password is reset via password recovery. This issue has been resolved in version 6.4.8.1. For older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin.	2.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22348	IBM Spectrum Protect Operations Center 8.1.0.000 through 8.1.13.xxx is vulnerable to reverse tabnabbing where it could allow a page linked to from within Operations Center to rewrite it. An administrator could enter a link to a malicious URL that another administrator could then click. Once clicked, that malicious URL could then rewrite the original page with a phishing page. IBM X-Force ID: 220139.	2.4	More Details
CVE-2022-25830	Information Exposure vulnerability in Galaxy Watch3 Plugin prior to version 2.2.09.22012751 allows attacker to access password information of connected WiFiAp in the log	1.9	More Details
CVE-2022-25823	Information Exposure vulnerability in Galaxy Watch Plugin prior to version 2.2.05.220126741 allows attackers to access user information in log.	1.9	More Details
CVE-2022-25826	Information Exposure vulnerability in Galaxy S3 Plugin prior to version 2.2.03.22012751 allows attacker to access password information of connected WiFiAp in the log	1.9	More Details
CVE-2022-25827	Information Exposure vulnerability in Galaxy Watch Plugin prior to version 2.2.05.22012751 allows attacker to access password information of connected WiFiAp in the log	1.9	More Details
CVE-2022-25828	Information Exposure vulnerability in Watch Active Plugin prior to version 2.2.07.22012751 allows attacker to access password information of connected WiFiAp in the log	1.9	More Details
CVE-2022-25829	Information Exposure vulnerability in Watch Active2 Plugin prior to version 2.2.08.22012751 allows attacker to access password information of connected WiFiAp in the log	1.9	More Details
CVE-2021-32501	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2022-26333	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2022-26351	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-26320. Reason: This candidate is a reservation duplicate of CVE-2022-26320. Notes: All CVE users should reference CVE-2022-26320 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32502	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-44597	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-43857. Reason: This candidate is a reservation duplicate of CVE-2021-43857. Notes: All CVE users should reference CVE-2021-43857 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2021-3558	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-2020-36123	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-2021-32505	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none	N/A	More Details
CVE-2021-42186	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