SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 04 May 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-2022-24900	Piano LED Visualizer is software that allows LED lights to light up as a person plays a piano connected to a computer. Version 1.3 and prior are vulnerable to a path traversal attack. The `os.path.join` call is unsafe for use with untrusted input. When the `os.path.join` call encounters an absolute path, it ignores all the parameters it has encountered till that point and starts working with the new absolute path. Since the "malicious" parameter represents an absolute path, the result of `os.path.join` ignores the static directory completely. Hence, untrusted input is passed via the `os.path.join` call to `flask.send_file` can lead to path traversal attacks. A patch with a fix is available on the `master` branch of the GitHub repository. This can also be fixed by preventing flow of untrusted data to the vulnerable `send_file` function. In case the application logic necessiates this behaviour, one can either use the `flask.safe_join` to join untrusted paths or replace `flask.send_file` calls with `flask.send_from_directory` calls.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1509	Command Injection Vulnerability in GitHub repository hestiacp/hestiacp prior to 1.5.12. An authenticated remote attacker with low privileges can execute arbitrary code under root context.	9.9	More Details
CVE-2022-1300	Multiple Version of TRUMPF TruTops products expose a service function without necessary authentication. Execution of this function may result in unauthorized access to change of data or disruption of the whole service.	9.8	More Details
CVE-2022-1371	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in ReadRegf. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-27982	RG-NBR-E Enterprise Gateway RG-NBR2100G-E was discovered to contain a remote code execution (RCE) vulnerability via the fileName parameter at /guest_auth/cfg/upLoadCfg.php.	9.8	More Details
CVE-2022-28054	Improper sanitization of trigger action scripts in VanDyke Software VShell for Windows v4.6.2 allows attackers to execute arbitrary code via a crafted value.	9.8	More Details
CVE-2022-28056	ShopXO v2.2.5 and below was discovered to contain a system re-install vulnerability via the Add function in app/install/controller/Index.php.	9.8	More Details
CVE-2022-28573	D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function SetNTPserverSeting. This vulnerability allows attackers to execute arbitrary commands via the system_time_timezone parameter.	9.8	More Details
CVE-2022-0771	The SiteSuperCharger WordPress plugin before 5.2.0 does not validate, sanitise and escape various user inputs before using them in SQL statements via AJAX actions (available to both unauthenticated and authenticated users), leading to Unauthenticated SQL Injections	9.8	More Details
CVE-2022-0773	The Documentor WordPress plugin through 1.5.3 fails to sanitize and escape user input before it is being interpolated in an SQL statement and then executed, leading to an SQL Injection exploitable by unauthenticated users.	9.8	More Details
CVE-2022-0783	The Multiple Shipping Address Woocommerce WordPress plugin before 2.0 does not properly sanitise and escape numerous parameters before using them in SQL statements via some AJAX actions available to unauthenticated users, leading to unauthenticated SQL injections	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1281	The Photo Gallery WordPress plugin through 1.6.3 does not properly escape the $_POST['filter_tag'] parameter, which is appended to an SQL query, making SQL Injection attacks possible.	9.8	More Details
CVE-2022-1366	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in HandlerChart.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-1367	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in Handler_TCV.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-1369	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in ReadRegIND. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-1370	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in ReadREGbyID. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-1372	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in dlSlog.aspx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-28571	D-link 882 DIR882A1_FW130B06 was discovered to contain a command injection vulnerability in`/usr/bin/cli.	9.8	More Details
CVE-2022-1374	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in DIAE_unHandler.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-1375	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in DIAE_slogHandler.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1376	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in DIAE_privgrpHandler.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-1377	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in DIAE_rltHandler.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2022-1378	Delta Electronics DIAEnergie (All versions prior to 1.8.02.004) has a blind SQL injection vulnerability exists in DIAE_pgHandler.ashx. This allows an attacker to inject arbitrary SQL queries, retrieve and modify database contents, and execute system commands.	9.8	More Details
CVE-2020-23620	The Java Remote Management Interface of all versions of Orlansoft ERP was discovered to contain a vulnerability due to insecure deserialization of user-supplied content, which can allow attackers to execute arbitrary code via a crafted serialized Java object.	9.8	More Details
CVE-2020-23621	The Java Remote Management Interface of all versions of SVI MS Management System was discovered to contain a vulnerability due to insecure deserialization of user-supplied content, which can allow attackers to execute arbitrary code via a crafted serialized Java object.	9.8	More Details
CVE-2022-28118	SiteServer CMS v7.x allows attackers to execute arbitrary code via a crafted plug-in.	9.8	More Details
CVE-2022-1292	The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).	9.8	More Details
CVE-2022-28560	There is a stack overflow vulnerability in the goform/fast_setting_wifi_set function in the httpd service of Tenda ac9 15.03.2.21_cn router. An attacker can obtain a stable shell through a carefully constructed payload	9.8	More Details
CVE-2022-28561	There is a stack overflow vulnerability in the /goform/setMacFilterCfg function in the httpd service of Tenda ax12 22.03.01.21_cn router. An attacker can obtain a stable shell through a carefully constructed payload	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27962	Bluecms 1.6 has a SQL injection vulnerability at cooike.	9.8	More Details
CVE-2022-28585	EmpireCMS 7.5 has a SQL injection vulnerability in AdClass.php	9.8	More Details
CVE-2022-27466	MCMS v5.2.27 was discovered to contain a SQL injection vulnerability in the orderBy parameter at /dict/list.do.	9.8	More Details
CVE-2022-27413	Hospital Management System v1.0 was discovered to contain a SQL injection vulnerability via the adminname parameter in admin.php.	9.8	More Details
CVE-2021-46442	In the "webupg" binary of D-Link DIR-825 G1, attackers can bypass authentication through parameters "autoupgrade.asp", and perform functions such as downloading configuration files and updating firmware without authorization.	9.8	More Details
CVE-2022-27336	Seacms v11.6 was discovered to contain a remote code execution (RCE) vulnerability via the component /admin/weixin.php.	9.8	More Details
CVE-2022-28719	Missing authentication for critical function in AssetView prior to Ver.13.2.0 allows a remote unauthenticated attacker with some knowledge on the system configuration to upload a crafted configuration file to the managing server, which may result in the managed clients to execute arbitrary code with the administrative privilege.	9.8	More Details
CVE-2021-41921	novel-plus V3.6.1 allows unrestricted file uploads. Unrestricted file suffixes and contents can lead to server attacks and arbitrary code execution.	9.8	More Details
CVE-2021-38869	IBM QRadar SIEM 7.3, 7.4, and 7.5 in some situations may not automatically log users out after they exceede their idle timeout. IBM X-Force ID: 208341.	9.8	More Details
CVE-2021-34601	In Bender/ebee Charge Controllers in multiple versions are prone to Hardcoded Credentials. Bender charge controller CC612 in version 5.20.1 and below is prone to hardcoded ssh credentials. An attacker may use the password to gain administrative access to the web-UI.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43934	Elcomplus SmartPTT is vulnerable as the backup and restore system does not adequately validate upload requests, enabling a malicious user to potentially upload arbitrary files.	9.8	More Details
CVE-2022-25767	All versions of package com.bstek.ureport:ureport2-console are vulnerable to Remote Code Execution by connecting to a malicious database server, causing arbitrary file read and deserialization of local gadgets.	9.8	More Details
CVE-2022-29081	Zoho ManageEngine Access Manager Plus before 4302, Password Manager Pro before 12007, and PAM360 before 5401 are vulnerable to access-control bypass on a few Rest API URLs (for SSOutAction. SSLAction. LicenseMgr. GetProductDetails. GetDashboard. FetchEvents. and Synchronize) via the ../RestAPI substring.	9.8	More Details
CVE-2022-29556	The iot-manager microservice 1.0.0 in Northern.tech Mender Enterprise before 3.2.2 allows SSRF because the Azure IoT Hub integration provides several SSRF primitives that can execute cross-tenant actions via internal API endpoints.	9.8	More Details
CVE-2022-24449	Solar appScreener through 3.10.4, when a valid license is not present, allows XXE and SSRF attacks via a crafted XML document.	9.8	More Details
CVE-2022-29904	The SemanticDrilldown extension for MediaWiki through 1.37.2 (before e688bdba6434591b5dff689a45e4d53459954773) allows SQL injection with certain '-' and '_' constraints.	9.8	More Details
CVE-2021-46422	Telesquare SDT-CW3B1 1.1.0 is affected by an OS command injection vulnerability that allows a remote attacker to execute OS commands without any authentication.	9.8	More Details
CVE-2022-29906	The admin API module in the QuizGame extension for MediaWiki through 1.37.2 (before 665e33a68f6fa1167df99c0aa18ed0157cdf9f66) omits a check for the quizadmin user.	9.8	More Details
CVE-2022-1531	SQL injection vulnerability in ARAX-UI Synonym Lookup functionality in GitHub repository rtxteam/rtx prior to checkpoint_2022-04-20 . This vulnerability is critical as it can lead to remote code execution and thus complete server takeover.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44596	Wondershare LTD Dr. Fone as of 2021-12-06 version is affected by Remote code execution. Due to software design flaws an unauthenticated user can communicate over UDP with the "InstallAssistService.exe" service(the service is running under SYSTEM privileges) and manipulate it to execute malicious executable without any validation from a remote location and gain SYSTEM privileges	9.8	More Details
CVE-2022-28452	Red Planet Laundry Management System 1.0 is vulnerable to SQL Injection.	9.8	More Details
CVE-2022-28480	ALLMediaServer 1.6 is vulnerable to Buffer Overflow via MediaServer.exe.	9.8	More Details
CVE-2022-28994	Small HTTP Server version 3.06 suffers from a remote buffer overflow vulnerability via long GET request.	9.8	More Details
CVE-2022-28481	CSV-Safe gem < 3.0.0 doesn't filter out special characters which could trigger CSV Injection.	9.8	More Details
CVE-2022-24437	The package git-pull-or-clone before 2.0.2 are vulnerable to Command Injection due to the use of the --upload-pack feature of git which is also supported for git clone. The source includes the use of the secure child process API spawn(). However, the outpath parameter passed to it may be a command-line argument to the git clone command and result in arbitrary command injection.	9.8	More Details
CVE-2022-29859	component/common/network/dhcp/dhcps.c in ambiot amb1_sdk (aka SDK for Ameba1) before 2022-03-11 mishandles data structures for DHCP packet data.	9.8	More Details
CVE-2021-46424	Telesquare TLR-2005KSH 1.0.0 is affected by an arbitrary file deletion vulnerability that allows a remote attacker to delete any file, even system internal files, via a DELETE request.	9.1	More Details
CVE-2022-28114	DSCMS v3.0 was discovered to contain an arbitrary file deletion vulnerability via /controller/Adv.php.	9.1	More Details
CVE-2021-41945	Encode OSS httpx < 0.23.0 is affected by improper input validation in `httpx.URL`, `httpx.Client` and some functions using `httpx.URL.copy_with`.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3643	A flaw was found in sox 14.4.1. The lsx_adpcm_init function within libsox leads to a global-buffer-overflow. This flaw allows an attacker to input a malicious file, leading to the disclosure of sensitive information.	9.1	More Details
CVE-2022-27332	An access control issue in Zammad v5.0.3 allows attackers to write entries to the CTI caller log without authentication. This vulnerability can allow attackers to execute phishing attacks or cause a Denial of Service (DoS).	9.1	More Details
CVE-2022-28101	Turtlapp Turtle Note v0.7.2.6 does not filter the <meta> tag during markdown parsing, allowing attackers to execute HTML injection.	9.0	More Details
CVE-2022-28464	Apifox through 2.1.6 is vulnerable to Cross Site Scripting (XSS) which can lead to remote code execution.	9.0	More Details
CVE-2021-43932	Elcomplus SmartPTT is vulnerable when an attacker injects JavaScript code into a specific parameter that can executed upon accessing the dashboard or the main page.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-23063	In Shopizer versions 2.3.0 to 3.0.1 are vulnerable to Insufficient Session Expiration. When a password has been changed by the user or by an administrator, a user that was already logged in, will still have access to the application even after the password was changed.	8.8	More Details
CVE-2022-28892	Mahara before 20.10.5, 21.04.4, 21.10.2, and 22.04.0 is vulnerable to Cross Site Request Forgery (CSRF) because randomly generated tokens are too easily guessable.	8.8	More Details
CVE-2021-36207	Under certain circumstances improper privilege management in Metasys ADS/ADX/OAS servers versions 10 and 11 could allow an authenticated user to elevate their privileges to administrator.	8.8	More Details
CVE-2022-22315	IBM UrbanCode Deploy (UCD) 7.2.2.1 could allow an authenticated user with special permissions to obtain elevated privileges due to improper handling of permissions. IBM X-Force ID: 217955.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1227	A privilege escalation flaw was found in Podman. This flaw allows an attacker to publish a malicious image to a public registry. Once this image is downloaded by a potential victim, the vulnerability is triggered after a user runs the 'podman top' command. This action gives the attacker access to the host filesystem, leading to information disclosure or denial of service.	8.8	More Details
CVE-2022-29451	Cross-Site Request Forgery (CSRF) leading to Arbitrary File Upload vulnerability in Rara One Click Demo Import plugin <= 1.2.9 on WordPress allows attackers to trick logged-in admin users into uploading dangerous files into /wp-content/uploads/ directory.	8.8	More Details
CVE-2022-29936	USU Oracle Optimization before 5.17 allows authenticated quantum users to achieve remote code execution because of /v2/quantum/save-data-upload-big-file Java deserialization. NOTE: this is not an Oracle Corporation product.	8.8	More Details
CVE-2022-29937	USU Oracle Optimization before 5.17.5 allows authenticated DataCollection users to achieve agent root access because some common OS commands are blocked but (for example) an OS command for base64 decoding is not blocked. NOTE: this is not an Oracle Corporation product.	8.8	More Details
CVE-2022-1543	Improper handling of Length parameter in GitHub repository erudika/scoold prior to 1.49.4. When the text size is large enough the service results in a momentary outage in a production environment. That can lead to memory corruption on the server.	8.8	More Details
CVE-2021-44595	Wondershare Dr. Fone Latest version as of 2021-12-06 is vulnerable to Incorrect Access Control. A normal user can send manually crafted packets to the ElevationService.exe and execute arbitrary code without any validation with SYSTEM privileges.	8.8	More Details
CVE-2022-29555	The Deviceconnect microservice through 1.3.0 in Northern.tech Mender Enterprise before 3.2.2. allows Cross-Origin Websocket Hijacking.	8.8	More Details
CVE-2022-23064	In Snipe-IT, versions v3.0-alpha to v5.3.7 are vulnerable to Host Header Injection. By sending a specially crafted host header in the reset password request, it is possible to send password reset links to users which once clicked lead to an attacker controlled server and thus leading to password reset token leak. This leads to account take over.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34602	In Bender/ebee Charge Controllers in multiple versions are prone to Command injection via Web interface. An authenticated attacker could enter shell commands into some input fields that are executed with root privileges.	8.8	More Details
CVE-2021-34592	In Bender/ebee Charge Controllers in multiple versions are prone to Command injection via Web interface. An authenticated attacker could enter shell commands into some input fields.	8.8	More Details
CVE-2022-28572	Tenda AX1806 v1.0.0.1 was discovered to contain a command injection vulnerability in `SetIPv6Status` function	8.8	More Details
CVE-2022-0952	The Sitemap by click5 WordPress plugin before 1.0.36 does not have authorisation and CSRF checks when updating options via a REST endpoint, and does not ensure that the option to be updated belongs to the plugin. As a result, unauthenticated attackers could change arbitrary blog options, such as the users_can_register and default_role, allowing them to create a new admin account and take over the blog.	8.8	More Details
CVE-2022-1239	The HubSpot WordPress plugin before 8.8.15 does not validate the proxy URL given to the proxy REST endpoint, which could allow users with the edit_posts capability (by default contributor and above) to perform SSRF attacks	8.8	More Details
CVE-2021-42165	MitraStar GPT-2541GNAC-N1 (HGU) 100VNZ0b33 devices allow remote authenticated users to obtain root access by executing command "deviceinfo show file &&/bin/bash" because of incorrect sanitization of parameter "path".	8.8	More Details
CVE-2021-46441	In the "webupg" binary of D-Link DIR-825 G1, because of the lack of parameter verification, attackers can use "cmd" parameters to execute arbitrary system commands after obtaining authorization.	8.8	More Details
CVE-2022-21949	A Improper Restriction of XML External Entity Reference vulnerability in SUSE Open Build Service allows remote attackers to reference external entities in certain operations. This can be used to gain information from the server that can be abused to escalate to Admin privileges on OBS. This issue affects: SUSE Open Build Service Open Build Service versions prior to 2.10.13.	8.8	More Details
CVE-2021-43939	Elcomplus SmartPTT is vulnerable when a low-authenticated user can access higher level administration authorization by issuing requests directly to the desired endpoints.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20759	A vulnerability in the web services interface for remote access VPN features of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, but unprivileged, remote attacker to elevate privileges to level 15. This vulnerability is due to improper separation of authentication and authorization scopes. An attacker could exploit this vulnerability by sending crafted HTTPS messages to the web services interface of an affected device. A successful exploit could allow the attacker to gain privilege level 15 access to the web management interface of the device. This includes privilege level 15 access to the device using management tools like the Cisco Adaptive Security Device Manager (ASDM) or the Cisco Security Manager (CSM). Note: With Cisco FTD Software, the impact is lower than the CVSS score suggests because the affected web management interface allows for read access only.	8.8	More Details
CVE-2021-22573	The vulnerability is that IDToken verifier does not verify if token is properly signed. Signature verification makes sure that the token's payload comes from valid provider, not from someone else. An attacker can provide a compromised token with custom payload. The token will pass the validation on the client side. We recommend upgrading to version 1.33.3 or above	8.7	More Details
CVE-2022-20745	A vulnerability in the web services interface for remote access VPN features of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper input validation when parsing HTTPS requests. An attacker could exploit this vulnerability by sending a crafted HTTPS request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2022-23923	All versions of package jailed are vulnerable to Sandbox Bypass via an exported alert() method which can access the main application. Exported methods are stored in the application.remote object.	8.6	More Details
CVE-2022-20760	A vulnerability in the DNS inspection handler of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service condition (DoS) on an affected device. This vulnerability is due to a lack of proper processing of incoming requests. An attacker could exploit this vulnerability by sending crafted DNS requests at a high rate to an affected device. A successful exploit could allow the attacker to cause the device to stop responding, resulting in a DoS condition.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20746	A vulnerability in the TCP proxy functionality of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to improper handling of TCP flows. An attacker could exploit this vulnerability by sending a crafted stream of TCP traffic through an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2022-20757	A vulnerability in the connection handling function in Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper traffic handling when platform limits are reached. An attacker could exploit this vulnerability by sending a high rate of UDP traffic through an affected device. A successful exploit could allow the attacker to cause all new, incoming connections to be dropped, resulting in a DoS condition.	8.6	More Details
CVE-2022-20751	A vulnerability in the Snort detection engine integration for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause unlimited memory consumption, which could lead to a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient memory management for certain Snort events. An attacker could exploit this vulnerability by sending a series of crafted IP packets that would generate specific Snort events on an affected device. A sustained attack could cause an out of memory condition on the affected device. A successful exploit could allow the attacker to interrupt all traffic flowing through the affected device. In some circumstances, the attacker may be able to cause the device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2022-20715	A vulnerability in the remote access SSL VPN features of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper validation of errors that are logged as a result of client connections that are made using remote access VPN. An attacker could exploit this vulnerability by sending crafted requests to an affected system. A successful exploit could allow the attacker to cause the affected device to restart, resulting in a DoS condition.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20767	A vulnerability in the Snort rule evaluation function of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper handling of the DNS reputation enforcement rule. An attacker could exploit this vulnerability by sending crafted UDP packets through an affected device to force a buildup of UDP connections. A successful exploit could allow the attacker to cause traffic that is going through the affected device to be dropped, resulting in a DoS condition. Note: This vulnerability only affects Cisco FTD devices that are running Snort 3.	8.6	More Details
CVE-2021-34588	In Bender/ebee Charge Controllers in multiple versions are prone to unprotected data export. Backup export is protected via a random key. The key is set at user login. It is empty after reboot .	8.6	More Details
CVE-2022-20737	A vulnerability in the handler for HTTP authentication for resources accessed through the Clientless SSL VPN portal of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device or to obtain portions of process memory from an affected device. This vulnerability is due to insufficient bounds checking when parsing specific HTTP authentication messages. An attacker could exploit this vulnerability by sending malicious traffic to an affected device acting as a VPN Gateway. To send this malicious traffic, an attacker would need to control a web server that can be accessed through the Clientless SSL VPN portal. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition, or to retrieve bytes from the device process memory that may contain sensitive information.	8.5	More Details
CVE-2022-0916	An issue was discovered in Logitech Options. The OAuth 2.0 state parameter was not properly validated. This leaves applications vulnerable to CSRF attacks during authentication and authorization operations.	8.4	More Details
CVE-2022-20111	In ion, there is a possible use after free due to incorrect error handling. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366069; Issue ID: ALPS06366069.	8.4	More Details
CVE-2022-29411	SQL Injection (SQLi) vulnerability in Mufeng's Hermit 音乐播放器 plugin <= 3.1.6 on WordPress allows attackers to execute SQLi attack via (&id).	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4207	A flaw was found in the QXL display device emulation in QEMU. A double fetch of guest controlled values `cursor->header.width` and `cursor->header.height` can lead to the allocation of a small cursor object followed by a subsequent heap-based buffer overflow. A malicious privileged guest user could use this flaw to crash the QEMU process on the host or potentially execute arbitrary code within the context of the QEMU process.	8.2	More Details
CVE-2021-4206	A flaw was found in the QXL display device emulation in QEMU. An integer overflow in the cursor_alloc() function can lead to the allocation of a small cursor object followed by a subsequent heap-based buffer overflow. This flaw allows a malicious privileged guest user to crash the QEMU process on the host or potentially execute arbitrary code within the context of the QEMU process.	8.2	More Details
CVE-2021-3750	A DMA reentrancy issue was found in the USB EHCI controller emulation of QEMU. EHCI does not verify if the Buffer Pointer overlaps with its MMIO region when it transfers the USB packets. Crafted content may be written to the controller's registers and trigger undesirable actions (such as reset) while the device is still transferring packets. This can ultimately lead to a use-after-free issue. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition, or potentially execute arbitrary code within the context of the QEMU process on the host. This flaw affects QEMU versions before 7.0.0.	8.2	More Details
CVE-2021-43938	Elcomplus SmartPTT SCADA Server is vulnerable to an unauthenticated user can request various files from the server without any authentication or authorization.	8.1	More Details
CVE-2021-42001	PingID Desktop prior to 1.7.3 has a misconfiguration in the encryption libraries which can lead to sensitive data exposure. An attacker capable of exploiting this vulnerability may be able to successfully complete an MFA challenge via OTP.	8.0	More Details
CVE-2022-23904	Rainworx Auctionworx < 3.1R2 is vulnerable to a Cross-Site Request Forgery (CSRF) attack that allows an authenticated user to upgrade his account to admin and gain access to the auctionworx admin control panel. This vulnerability affects AuctionWorx Enterprise and AuctionWorx: Events Edition.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22782	The Zoom Client for Meetings for Windows prior to version 5.9.7, Zoom Rooms for Conference Room for Windows prior to version 5.10.0, Zoom Plugins for Microsoft Outlook for Windows prior to version 5.10.3, and Zoom VDI Windows Meeting Clients prior to version 5.9.6; was susceptible to a local privilege escalation issue during the installer repair operation. A malicious actor could utilize this to potentially delete system level files or folders, causing integrity or availability issues on the user's host machine.	7.9	More Details
CVE-2022-1533	Buffer Over-read in GitHub repository bfabiszewski/libmobi prior to 0.11. This vulnerability is capable of arbitrary code execution.	7.8	More Details
CVE-2022-20088	In aee driver, there is a possible reference count mistake due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06209201.	7.8	More Details
CVE-2022-20093	In telephony, there is a possible way to disable receiving SMS messages 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: ALPS06498868; Issue ID: ALPS06498868.	7.8	More Details
CVE-2021-46790	ntfsck in NTFS-3G through 2021.8.22 has a heap-based buffer overflow involving buffer+512*3-2. NOTE: the upstream position is that ntfsck is deprecated; however, it is shipped by some Linux distributions.	7.8	More Details
CVE-2022-20084	In telephony, there is a possible way to disable receiving emergency broadcasts 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: ALPS06498874; Issue ID: ALPS06498874.	7.8	More Details
CVE-2022-1402	ASDA-Soft: Version 5.4.1.0 and prior does not properly sanitize input while processing a specific project file, allowing a possible out-of-bounds read condition.	7.8	More Details
CVE-2022-1403	ASDA-Soft: Version 5.4.1.0 and prior does not properly sanitize input while processing a specific project file, allowing a possible out-of-bounds write condition.	7.8	More Details
CVE-2022-29934	USU Oracle Optimization before 5.17.5 lacks Polkit authentication, which allows smartcollector users to achieve root access via pkexec. NOTE: this is not an Oracle Corporation product.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1544	Formula Injection/CSV Injection due to Improper Neutralization of Formula Elements in CSV File in GitHub repository luyadev/yii-helpers prior to 1.2.1. Successful exploitation can lead to impacts such as client-sided command injection, code execution, or remote ex-filtration of contained confidential data.	7.8	More Details
CVE-2022-29849	In Progress OpenEdge before 11.7.14 and 12.x before 12.2.9, certain SUID binaries within the OpenEdge application were susceptible to privilege escalation. If exploited, a local attacker could elevate their privileges and compromise the affected system.	7.8	More Details
CVE-2022-29968	An issue was discovered in the Linux kernel through 5.17.5. io_rw_init_file in fs/io_uring.c lacks initialization of kiocb->private.	7.8	More Details
CVE-2022-20109	In ion, there is a possible use after free due to improper update of reference count. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399915.	7.8	More Details
CVE-2021-42529	XMP Toolkit SDK version 2021.07 (and earlier) is affected by a stack-based buffer overflow vulnerability 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.	7.8	More Details
CVE-2021-42530	XMP Toolkit SDK version 2021.07 (and earlier) is affected by a stack-based buffer overflow vulnerability 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.	7.8	More Details
CVE-2021-42531	XMP Toolkit SDK version 2021.07 (and earlier) is affected by a stack-based buffer overflow vulnerability 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.	7.8	More Details
CVE-2021-42532	XMP Toolkit SDK version 2021.07 (and earlier) is affected by a stack-based buffer overflow vulnerability 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.	7.8	More Details
CVE-2022-20099	In aee daemon, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296442.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21743	In ion, there is a possible use after free due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06371108; Issue ID: ALPS06371108.	7.8	More Details
CVE-2022-27239	In cifs-utils through 6.14, a stack-based buffer overflow when parsing the mount.cifs ip= command-line argument could lead to local attackers gaining root privileges.	7.8	More Details
CVE-2021-34591	In Bender/ebee Charge Controllers in multiple versions are prone to Local privilege Escalation. An authenticated attacker could get root access via the suid applications socat, ip udhcpc and ifplugd.	7.8	More Details
CVE-2022-28085	A flaw was found in htmldoc commit 31f7804. A heap buffer overflow in the function pdf_write_names in ps-pdf.cxx may lead to arbitrary code execution and Denial of Service (DoS).	7.8	More Details
CVE-2022-29505	Due to build misconfiguration in openssl dependency, LINE for Windows before 7.8 is vulnerable to DLL injection that could lead to privilege escalation.	7.8	More Details
CVE-2022-25647	The package com.google.code.gson:gson before 2.8.9 are vulnerable to Deserialization of Untrusted Data via the writeReplace() method in internal classes, which may lead to DoS attacks.	7.7	More Details
CVE-2022-25301	All versions of package jsgui-lang-essentials are vulnerable to Prototype Pollution due to allowing all Object attributes to be altered, including their magical attributes such as proto, constructor and prototype.	7.7	More Details
CVE-2022-23723	An MFA bypass vulnerability exists in the PingFederate PingOne MFA Integration Kit when adapter HTML templates are used as part of an authentication flow.	7.7	More Details
CVE-2022-28781	Improper input validation in Settings prior to SMR-May-2022 Release 1 allows attackers to launch arbitrary activity with system privilege. The patch adds proper validation logic to check the caller.	7.7	More Details
CVE-2021-41992	A misconfiguration of RSA in PingID Windows Login prior to 2.7 is vulnerable to pre-computed dictionary attacks, leading to an offline MFA bypass.	7.7	More Details
CVE-2021-43937	Elcomplus SmartPTT SCADA Server web application does not, or cannot, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22278	A vulnerability in SonicOS CFS (Content filtering service) returns a large 403 forbidden HTTP response message to the source address when users try to access prohibited resource this allows an attacker to cause HTTP Denial of Service (DoS) attack	7.5	More Details
CVE-2022-28060	SQL Injection vulnerability in Victor CMS v1.0, via the user_name parameter to /includes/login.php.	7.5	More Details
CVE-2022-29265	Multiple components in Apache NiFi 0.0.1 to 1.16.0 do not restrict XML External Entity references in the default configuration. The Standard Content Viewer service attempts to resolve XML External Entity references when viewing formatted XML files. The following Processors attempt to resolve XML External Entity references when configured with default property values: - EvaluateXPath - EvaluateXQuery - ValidateXml Apache NiFi flow configurations that include these Processors are vulnerable to malicious XML documents that contain Document Type Declarations with XML External Entity references. The resolution disables Document Type Declarations in the default configuration for these Processors, and disallows XML External Entity resolution in standard services.	7.5	More Details
CVE-2022-29967	static_compressed_inmemory_website_callback.c in Glewlwyd through 2.6.2 allows directory traversal.	7.5	More Details
CVE-2021-38919	IBM QRadar SIEM 7.3, 7.4, and 7.5 in some senarios may reveal authorized service tokens to other QRadar users. IBM X-Force ID: 210021	7.5	More Details
CVE-2022-29970	Sinatra before 2.2.0 does not validate that the expanded path matches public_dir when serving static files.	7.5	More Details
CVE-2021-3523	A flaw was found in 3Scale APICast in versions prior to 2.11.0, where it incorrectly identified connections for reuse. This flaw allows an attacker to bypass security restrictions for an API request when hosting multiple APIs on the same IP address.	7.5	More Details
CVE-2021-41942	The Magic CMS MSVOD v10 video system has a SQL injection vulnerability. Attackers can use vulnerabilities to obtain sensitive information in the database.	7.5	More Details
CVE-2022-28451	nopCommerce 4.50.1 is vulnerable to Directory Traversal via the backup file in the Maintenance feature.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40822	GeoServer through 2.18.5 and 2.19.x through 2.19.2 allows SSRF via the option for setting a proxy host.	7.5	More Details
CVE-2021-39082	IBM UrbanCode Deploy (UCD) 7.1.1.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	7.5	More Details
CVE-2022-28323	An issue was discovered in MediaWiki through 1.37.2. The SecurePoll extension allows a leak because sorting by timestamp is supported,	7.5	More Details
CVE-2022-21144	This affects all versions of package libxmljs. When invoking the libxmljs.parseXml function with a non-buffer argument the V8 code will attempt invoking the .toString method of the argument. If the argument's toString value is not a Function object V8 will crash.	7.5	More Details
CVE-2022-22275	Improper Restriction of TCP Communication Channel in HTTP/S inbound traffic from WAN to DMZ bypassing security policy until TCP handshake potentially resulting in Denial of Service (DoS) attack if a target host is vulnerable.	7.5	More Details
CVE-2022-25850	The package github.com/hoppscotch/proxyscotch before 1.0.0 are vulnerable to Server-side Request Forgery (SSRF) when interceptor mode is set to proxy. It occurs when an HTTP request is made by a backend server to an untrusted URL submitted by a user. It leads to a leakage of sensitive information from the server.	7.5	More Details
CVE-2022-29935	USU Oracle Optimization before 5.17.5 allows attackers to discover the quantum credentials via an agent-installer download. NOTE: this is not an Oracle Corporation product.	7.5	More Details
CVE-2022-27983	RG-NBR-E Enterprise Gateway RG-NBR2100G-E was discovered to contain an arbitrary file read vulnerability via the url parameter in check.php.	7.5	More Details
CVE-2022-22143	The package convict before 6.2.2 are vulnerable to Prototype Pollution via the convict function due to missing validation of parentKey. **Note:** This vulnerability derives from an incomplete fix of another [vulnerability] (https://security.snyk.io/vuln/SNYK-JS-CONVICT-1062508)	7.5	More Details
CVE-2022-21227	The package sqlite3 before 5.0.3 are vulnerable to Denial of Service (DoS) which will invoke the toString function of the passed parameter. If passed an invalid Function object it will throw and crash the V8 engine.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27313	An arbitrary file deletion vulnerability in Gitea v1.16.3 allows attackers to cause a Denial of Service (DoS) via deleting the configuration file.	7.5	More Details
CVE-2022-29856	A hardcoded cryptographic key in Automation360 22 allows an attacker to decrypt exported RPA packages.	7.5	More Details
CVE-2022-21167	All versions of package masuit.tools.core are vulnerable to Arbitrary Code Execution via the ReceiveVarData<T> function in the SocketClient.cs component. The socket client in the package can pass in the payload via the user-controllable input after it has been established, because this socket client transmission does not have the appropriate restrictions or type bindings for the BinaryFormatter.	7.5	More Details
CVE-2021-41959	JerryScript Git version 14ff5bf does not sufficiently track and release allocated memory via jerry-core/ecma/operations/ecma-regexp-object.c after RegExp, which causes a memory leak.	7.5	More Details
CVE-2021-38878	IBM QRadar 7.3, 7.4, and 7.5 could allow a malicious actor to impersonate an actor due to key exchange without entity authentication. IBM X-Force ID: 208756.	7.5	More Details
CVE-2022-22368	IBM Spectrum Scale 5.1.0 through 5.1.3.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 221012.	7.5	More Details
CVE-2021-25002	The Tipsacarrier WordPress plugin before 1.5.0.5 does not have any authorisation check in place some functions, which could allow unauthenticated users to access Orders data which could be used to retrieve the client full address, name and phone via tracking URL	7.5	More Details
CVE-2022-28613	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is en-abled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500, causing the receiving RTU500 CMU to reboot. The vulnerability is caused by the validation error in the length information carried in MBAP header in the HCI Modbus TCP function.	7.5	More Details
CVE-2022-1554	Path Traversal due to `send_file` call in GitHub repository clinical-genomics/scout prior to 4.52.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46421	Franklin Fueling Systems FFS T5 Series 1.8.7.7299 is affected by an unauthenticated directory traversal vulnerability, which allows an attacker to obtain sensitive information.	7.5	More Details
CVE-2022-24879	Shopware is an open source e-commerce software platform. Versions prior to 5.7.9 are vulnerable to malfunction of cross-site request forgery (CSRF) token validation. Under certain circumstances, the CSRF tokens were not generated anew and not validated correctly. This issue is fixed in version 5.7.9. Users of older versions may attempt to mitigate the vulnerability by using the Shopware security plugin.	7.5	More Details
CVE-2022-29585	In Mahara before 20.10.5, 21.04.4, 21.10.2, and 22.04.0, a site using Isolated Institutions is vulnerable if more than ten groups are used. They are all shown from page 2 of the group results list (rather than only being shown for the institution that the viewer is a member of).	7.5	More Details
CVE-2021-42218	OMPL v1.5.2 contains a memory leak in VFRRT.cpp	7.5	More Details
CVE-2021-46440	Storing passwords in a recoverable format in the DOCUMENTATION plugin component of Strapi before 3.6.9 and 4.x before 4.1.5 allows an attacker to access a victim's HTTP request, get the victim's cookie, perform a base64 decode on the victim's cookie, and obtain a cleartext password, leading to getting API documentation for further API attacks.	7.5	More Details
CVE-2022-24935	Lexmark products through 2022-02-10 have Incorrect Access Control.	7.5	More Details
CVE-2021-46420	Franklin Fueling Systems FFS TS-550 evo 2.23.4.8936 is affected by an unauthenticated directory traversal vulnerability, which allows an attacker to obtain sensitive information.	7.5	More Details
CVE-2022-29700	A lack of password length restriction in Zammad v5.1.0 allows for the creation of extremely long passwords which can cause a Denial of Service (DoS) during password verification.	7.5	More Details
CVE-2021-34589	In Bender/ebee Charge Controllers in multiple versions are prone to an RFID leak. The RFID of the last charge event can be read without authentication via the web interface.	7.5	More Details
CVE-2022-22781	The Zoom Client for Meetings for MacOS (Standard and for IT Admin) prior to version 5.9.6 failed to properly check the package version during the update process. This could lead to a malicious actor updating an unsuspecting user’s currently installed version to a less secure version.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1473	The OPENSSL_LH_flush() function, which empties a hash table, contains a bug that breaks reuse of the memory occuppied by the removed hash table entries. This function is used when decoding certificates or keys. If a long lived process periodically decodes certificates or keys its memory usage will expand without bounds and the process might be terminated by the operating system causing a denial of service. Also traversing the empty hash table entries will take increasingly more time. Typically such long lived processes might be TLS clients or TLS servers configured to accept client certificate authentication. The function was added in the OpenSSL 3.0 version thus older releases are not affected by the issue. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2).	7.5	More Details
CVE-2022-29701	A lack of rate limiting in the 'forgot password' feature of Zammad v5.1.0 allows attackers to send an excessive amount of reset requests for a legitimate user, leading to a possible Denial of Service (DoS) via a large amount of generated e-mail messages.	7.5	More Details
CVE-2022-24897	APIs to evaluate content with Velocity is a package for APIs to evaluate content with Velocity. Starting with version 2.3 and prior to 12.6.7, 12.10.3, and 13.0, the velocity scripts are not properly sandboxed against using the Java File API to perform read or write operations on the filesystem. Writing an attacking script in Velocity requires the Script rights in XWiki so not all users can use it, and it also requires finding an XWiki API which returns a File. The problem has been patched in versions 12.6.7, 12.10.3, and 13.0. There is no easy workaround for fixing this vulnerability other than upgrading and being careful when giving Script rights.	7.5	More Details
CVE-2022-20742	A vulnerability in an IPsec VPN library of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to read or modify data within an IPsec IKEv2 VPN tunnel. This vulnerability is due to an improper implementation of Galois/Counter Mode (GCM) ciphers. An attacker in a man-in-the-middle position could exploit this vulnerability by intercepting a sufficient number of encrypted messages across an affected IPsec IKEv2 VPN tunnel and then using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to decrypt, read, modify, and re-encrypt data that is transmitted across an affected IPsec IKEv2 VPN tunnel.	7.4	More Details
CVE-2022-29410	Authenticated SQL Injection (SQLi) vulnerability in Mufeng's Hermit 音乐播放器 plugin <= 3.1.6 on WordPress allows attackers with Subscriber or higher user roles to execute SQLi attack via (&ids).	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22680	NXP MQX Versions 5.1 and prior are vulnerable to integer overflow in mem_alloc, _lwmem_alloc and _partition functions. This unverified memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	7.3	More Details
CVE-2021-27425	Cesanta Software Mongoose-OS v2.17.0 is vulnerable to integer wrap-around in function mm_malloc. This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	7.3	More Details
CVE-2021-27419	uClibc-ng versions prior to 1.0.37 are vulnerable to integer wrap-around in functions malloc-simple. This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	7.3	More Details
CVE-2022-28194	NVIDIA Jetson Linux Driver Package contains a vulnerability in the Cboot module tegrabl_cbo.c, where, if TFTP is enabled, a local attacker with elevated privileges can cause a memory buffer overflow, which may lead to code execution, loss of Integrity, limited denial of service, and some impact to confidentiality.	7.3	More Details
CVE-2021-33436	NoMachine for Windows prior to version 6.15.1 and 7.5.2 suffer from local privilege escalation due to the lack of safe DLL loading. This vulnerability allows local non-privileged users to perform DLL Hijacking via any writable directory listed under the system path and ultimately execute code as NT AUTHORITY\SYSTEM.	7.3	More Details
CVE-2021-27421	NXP MCUXpresso SDK versions prior to 2.8.2 are vulnerable to integer overflow in SDK_Malloc function, which could allow to access memory locations outside the bounds of a specified array, leading to unexpected behavior such segmentation fault when assigning a particular block of memory from the heap via malloc.	7.3	More Details
CVE-2022-22521	In Miele Benchmark Programming Tool with versions Prior to 1.2.71, executable files manipulated by attackers are unknowingly executed with users privileges. An attacker with low privileges may trick a user with administrative privileges to execute these binaries as admin.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21189	The package dexie before 3.2.2, from 4.0.0-alpha.1 and before 4.0.0-alpha.3 are vulnerable to Prototype Pollution in the Dexie.setByKeyPath(obj, keyPath, value) function which does not properly check the keys being set (like __proto__ or constructor). This can allow an attacker to add/modify properties of the Object.prototype leading to prototype pollution vulnerability. **Note:** This vulnerability can occur in multiple ways, for example when modifying a collection with untrusted user input.	7.3	More Details
CVE-2021-27427	RIOT OS version 2020.01.1 is vulnerable to integer wrap-around in its implementation of calloc function, which can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	7.3	More Details
CVE-2021-27439	TencentOS-tiny version 3.1.0 is vulnerable to integer wrap-around in function 'tos_mmheap_alloc incorrect calculation of effective memory allocation size. This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	7.3	More Details
CVE-2021-27435	ARM mbed product Version 6.3.0 is vulnerable to integer wrap-around in malloc_wrapper function, which can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	7.3	More Details
CVE-2021-27433	ARM mbed-ualloc memory library version 1.3.0 is vulnerable to integer wrap-around in function mbed_krbs, which can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution.	7.3	More Details
CVE-2021-27431	ARM CMSIS RTOS2 versions prior to 2.1.3 are vulnerable to integer wrap-around inosRtxMemoryAlloc (local malloc equivalent) function, which can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or injected code execution.	7.3	More Details
CVE-2021-36778	A Incorrect Authorization vulnerability in SUSE Rancher allows administrators of third-party repositories to gather credentials that are sent to their servers. This issue affects: SUSE Rancher Rancher versions prior to 2.5.12; Rancher versions prior to 2.6.3.	7.3	More Details
CVE-2021-36784	A Improper Privilege Management vulnerability in SUSE Rancher allows users with the restricted-admin role to escalate to full admin. This issue affects: SUSE Rancher Rancher versions prior to 2.5.13; Rancher versions prior to 2.6.4.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27905	In ControlUp Real-Time Agent before 8.6, an unquoted path can result in privilege escalation. An attacker would require write permissions to the root level of the OS drive (C:\) to exploit this.	7.2	More Details
CVE-2021-29854	IBM Maximo Asset Management 7.6.1.1 and 7.6.1.2 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. By sending a specially crafted HTTP request, a remote attacker could exploit this vulnerability to inject HTTP HOST header, which will allow the attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 205680.	7.2	More Details
CVE-2022-1273	The Import WP WordPress plugin before 2.4.6 does not validate the imported file in some cases, allowing high privilege users such as admin to upload arbitrary files (such as PHP), leading to RCE	7.2	More Details
CVE-2022-28590	A Remote Code Execution (RCE) vulnerability exists in Pixelimity 1.0 via admin/admin-ajax.php?action=install_theme.	7.2	More Details
CVE-2022-29001	In SpringBootMovie <=1.2, the uploaded file suffix parameter is not filtered, resulting in arbitrary file upload vulnerability	7.2	More Details
CVE-2022-28505	Jfinal_cms 5.1.0 is vulnerable to SQL Injection via com.jflyfox.system.log.LogController.java.	7.2	More Details
CVE-2022-1353	A vulnerability was found in the pfkey_register function in net/key/af_key.c in the Linux kernel. This flaw allows a local, unprivileged user to gain access to kernel memory, leading to a system crash or a leak of internal kernel information.	7.1	More Details
CVE-2022-23400	A stack-based buffer overflow vulnerability exists in the IGXMPXMLParser::parseDelimiter functionality of Accusoft ImageGear 19.10. A specially-crafted PSD file can overflow a stack buffer, which could either lead to denial of service or, depending on the application, to an information leak. An attacker can provide a malicious file to trigger this vulnerability.	7.1	More Details
CVE-2022-1534	Buffer Over-read at parse_rawml.c:1416 in GitHub repository bfabiszewski/libmobi prior to 0.11. The bug causes the program reads data past the end of the intented buffer. Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1114	A heap-use-after-free flaw was found in ImageMagick's RelinquishDCMInfo() function of dcm.c file. This vulnerability is triggered when an attacker passes a specially crafted DICOM image file to ImageMagick for conversion, potentially leading to information disclosure and a denial of service.	7.1	More Details
CVE-2022-20110	In ion, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06399915; Issue ID: ALPS06399901.	7.0	More Details
CVE-2022-1048	A use-after-free flaw was found in the Linux kernel’s sound subsystem in the way a user triggers concurrent calls of PCM hw_params. The hw_free ioctls or similar race condition happens inside ALSA PCM for other ioctls. This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.0	More Details
CVE-2022-29819	In JetBrains IntelliJ IDEA before 2022.1 local code execution via links in Quick Documentation was possible	6.9	More Details
CVE-2022-29815	In JetBrains IntelliJ IDEA before 2022.1 local code execution via workspace settings was possible	6.9	More Details
CVE-2022-25842	All versions of package com.alibaba.oneagent:one-java-agent-plugin are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip) using a specially crafted archive that holds directory traversal filenames (e.g. ../../evil.exe). The attacker can overwrite executable files and either invoke them remotely or wait for the system or user to call them, thus achieving remote command execution on the victim’s machine.	6.9	More Details
CVE-2022-29821	In JetBrains Rider before 2022.1 local code execution via links in ReSharper Quick Documentation was possible	6.9	More Details
CVE-2022-29814	In JetBrains IntelliJ IDEA before 2022.1 local code execution via HTML descriptions in custom JSON schemas was possible	6.9	More Details
CVE-2022-29813	In JetBrains IntelliJ IDEA before 2022.1 local code execution via custom Pandoc path was possible	6.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29859	IBM ICP4A - User Management System Component (IBM Cloud Pak for Business Automation V21.0.3 through V21.0.3-IF008, V21.0.2 through V21.0.2-IF009, and V21.0.1 through V21.0.1-IF007) could allow a user with physical access to the system to perform unauthorized actions or obtain sensitive information due to insufficient validation and recvocation another user logouting out. IBM X-Force ID: 206081.	6.8	More Details
CVE-2022-23822	In this physical attack, an attacker may potentially exploit the Zynq-7000 SoC First Stage Boot Loader (FSBL) by bypassing authentication and loading a malicious image onto the device. This in turn may further allow the attacker to perform additional attacks such as such as using the device as a decryption oracle. An anticipated mitigation via a 2022.1 patch will resolve the issue.	6.8	More Details
CVE-2022-20106	In MM service, there is a possible out of bounds write due to a heap-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.	6.7	More Details
CVE-2022-20089	In aee driver, there is a possible memory corruption due to active debug code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06240397; Issue ID: ALPS06240397.	6.7	More Details
CVE-2022-20087	In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06477970; Issue ID: ALPS06477970.	6.7	More Details
CVE-2022-20108	In voice service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330702; Issue ID: DTV03330702.	6.7	More Details
CVE-2022-20095	In imgsensor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479763.	6.7	More Details
CVE-2022-20085	In netdiag, there is a possible symbolic link following due to an 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: ALPS06308877; Issue ID: ALPS06308877.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20094	In imgsensor, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479763; Issue ID: ALPS06479734.	6.7	More Details
CVE-2022-20105	In MM service, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330460; Issue ID: DTV03330460.	6.7	More Details
CVE-2022-28198	NVIDIA Omniverse Nucleus and Cache contain a vulnerability in its configuration of OpenSSL, where an attacker with physical access to the system can cause arbitrary code execution which can impact confidentiality, integrity, and availability.	6.6	More Details
CVE-2021-41994	A misconfiguration of RSA in PingID iOS app prior to 1.19 is vulnerable to pre-computed dictionary attacks, leading to an offline MFA bypass when using PingID Windows Login.	6.6	More Details
CVE-2022-1015	A flaw was found in the Linux kernel in linux/net/netfilter/nf_tables_api.c of the netfilter subsystem. This flaw allows a local user to cause an out-of-bounds write issue.	6.6	More Details
CVE-2021-41993	A misconfiguration of RSA in PingID Android app prior to 1.19 is vulnerable to pre-computed dictionary attacks, leading to an offline MFA bypass when using PingID Windows Login.	6.6	More Details
CVE-2022-22137	A memory corruption vulnerability exists in the ioca_mys_rgb_allocate functionality of Accusoft ImageGear 19.10. A specially-crafted malformed file can lead to an arbitrary free. An attacker can provide a malicious file to trigger this vulnerability.	6.5	More Details
CVE-2022-20743	A vulnerability in the web management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to bypass security protections and upload malicious files to the affected system. This vulnerability is due to improper validation of files uploaded to the web management interface of Cisco FMC Software. An attacker could exploit this vulnerability by uploading a maliciously crafted file to a device running affected software. A successful exploit could allow the attacker to store malicious files on the device, which they could access later to conduct additional attacks, including executing arbitrary code on the affected device with root privileges.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20744	A vulnerability in the input protection mechanisms of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to view data without proper authorization. This vulnerability exists because of a protection mechanism that relies on the existence or values of a specific input. An attacker could exploit this vulnerability by modifying this input to bypass the protection mechanism and sending a crafted request to an affected device. A successful exploit could allow the attacker to view data beyond the scope of their authorization.	6.5	More Details
CVE-2022-1511	Missing Authorization in GitHub repository snipe/snipe-it prior to 5.4.4.	6.5	More Details
CVE-2022-0191	The Ad Invalid Click Protector (AICP) WordPress plugin before 1.2.7 does not have CSRF check deleting banned users, which could allow attackers to make a logged in admin remove arbitrary bans	6.5	More Details
CVE-2022-22783	A vulnerability in Zoom On-Premise Meeting Connector Controller version 4.8.102.20220310 and On-Premise Meeting Connector MMR version 4.8.102.20220310 exposes process memory fragments to connected clients, which could be observed by a passive attacker.	6.5	More Details
CVE-2022-22312	IBM Security Identity Manager (IBM Security Verify Password Synchronization Plug-in for Windows AD 10.x) is vulnerable to a denial of service, caused by a heap-based buffer overflow in the Password Synch Plug-in. An authenticated attacker could exploit this vulnerability to cause a denial of service. IBM X-Force ID: 217369.	6.5	More Details
CVE-2022-23722	When a password reset mechanism is configured to use the Authentication API with an Authentication Policy, email One-Time Password, PingID or SMS authentication, an existing user can reset another existing user’s password.	6.5	More Details
CVE-2022-26068	This affects the package pistacheio/pistache before 0.0.3.20220425. It is possible to traverse directories to fetch arbitrary files from the server.	6.5	More Details
CVE-2022-22323	IBM Security Identity Manager (IBM Security Verify Password Synchronization Plug-in for Windows AD 10.x) is vulnerable to a denial of service, caused by a heap-based buffer overflow in the Password Synch Plug-in. An authenticated attacker could exploit this vulnerability to cause a denial of service. IBM X-Force ID: 218379.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27411	Micrium OS Versions 5.10.1 and prior are vulnerable to integer wrap-around in functions Mem_DynPoolCreate, Mem_DynPoolCreateHW and Mem_PoolCreate. This unverified memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as very small blocks of memory being allocated instead of very large ones.	6.5	More Details
CVE-2022-29444	Plugin Settings Change leading to Cross-Site Scripting (XSS) vulnerability in Cloudways Breeze plugin <= 2.0.2 on WordPress allows users with a subscriber or higher user role to execute any of the wp_ajax_* actions in the class Breeze_Configuration which includes the ability to change any of the plugin's settings including CDN setting which could be further used for XSS attack.	6.5	More Details
CVE-2022-23061	In Shopizer versions 2.0 to 2.17.0 a regular admin can permanently delete a superadmin (although this cannot happen according to the documentation) via Insecure Direct Object Reference (IDOR) vulnerability.	6.5	More Details
CVE-2022-29824	In libxml2 before 2.9.14, several buffer handling functions in buf.c (xmlBuf*) and tree.c (xmlBuffer*) don't check for integer overflows. This can result in out-of-bounds memory writes. Exploitation requires a victim to open a crafted, multi-gigabyte XML file. Other software using libxml2's buffer functions, for example libxslt through 1.1.35, is affected as well.	6.5	More Details
CVE-2022-25645	All versions of package dset are vulnerable to Prototype Pollution via 'dset/merge' mode, as the dset function checks for prototype pollution by validating if the top-level path contains __proto__, constructor or protorype. By crafting a malicious object, it is possible to bypass this check and achieve prototype pollution.	6.5	More Details
CVE-2022-22441	IBM InfoSphere Information Server 11.7 could allow an authenticated user to view information of higher privileged users and groups due to a privilege escalation vulnerability. IBM X-Force ID: 224426.	6.5	More Details
CVE-2022-24892	Shopware is an open source e-commerce software platform. Starting with version 5.0.4 and before version 5.7.9, multiple tokens for password reset can be requested. All tokens can be used to change the password. This makes it possible for an attacker to take over the victim's account if they somehow gain access to the victims email account and find an unused password reset token in the emails. This issue is fixed in version 5.7.9.	6.4	More Details
CVE-2022-20090	In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209197; Issue ID: ALPS06209197.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20091	In aee driver, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06209201; Issue ID: ALPS06226345.	6.4	More Details
CVE-2022-28792	DLL hijacking vulnerability in Gear IconX PC Manager prior to version 2.1.220405.51 allows attacker to execute arbitrary code. The patch adds proper absolute path to prevent dll hijacking.	6.2	More Details
CVE-2022-28789	Unprotected activities in Voice Note prior to version 21.3.51.11 allows attackers to record voice without user interaction. The patch adds proper permission for vulnerable activities.	6.2	More Details
CVE-2022-28791	Improper input validation vulnerability in InstallAgent in Galaxy Store prior to version 4.5.41.8 allows attacker to overwrite files stored in a specific path. The patch adds proper protection to prevent overwrite to existing files.	6.2	More Details
CVE-2022-28783	Improper validation of removing package name in Galaxy Themes prior to SMR May-2022 Release 1 allows attackers to uninstall arbitrary packages without permission. The patch adds proper validation logic for removing package name.	6.2	More Details
CVE-2022-27860	Cross-Site Request Forgery (CSRF) leading to Cross-Site Scripting (XSS) in Shea Bunge's Footer Text plugin <= 2.0.3 on WordPress.	6.1	More Details
CVE-2022-1250	The LifterLMS PayPal WordPress plugin before 1.4.0 does not sanitise and escape some parameters from the payment confirmation page before outputting them back in the page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2022-1269	The Fast Flow WordPress plugin before 1.2.12 does not sanitise and escape the page parameter before outputting back in an attribute in an admin dashboard, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-22427	IBM InfoSphere Information Server 11.7 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: 223720.	6.1	More Details
CVE-2020-23618	A reflected cross site scripting (XSS) vulnerability in Xtend Voice Logger 1.0 allows attackers to execute arbitrary web scripts or HTML, via the path of the error page.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1282	The Photo Gallery by 10Web WordPress plugin before 1.6.3 does not properly sanitize the $_GET['image_url'] variable, which is reflected back to the users when executing the editimage_bwg AJAX action.	6.1	More Details
CVE-2022-29415	Unauthenticated Reflected Cross-Site Scripting (XSS) vulnerability in Mati Skiba @ Rav Messer's Ravpage plugin <= 2.16 at WordPress.	6.1	More Details
CVE-2022-29947	Woodpecker before 0.15.1 allows XSS via build logs because web/src/components/repo/build/BuildLog.vue lacks escaping.	6.1	More Details
CVE-2022-0428	The Content Egg WordPress plugin before 5.3.0 does not sanitise and escape the page parameter before outputting back in an attribute in the Autoblogging admin dashboard, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-1530	Cross-site Scripting (XSS) in GitHub repository livehelperchat/livehelperchat prior to 3.99v. The attacker can execute malicious JavaScript on the application.	6.1	More Details
CVE-2022-29152	The Ericom PowerTerm WebConnect 6.0 login portal can unsafely write an XSS payload from the AppPortal cookie into the page.	6.1	More Details
CVE-2022-1504	XSS in /demo/module/?module=HERE in GitHub repository microweber/microweber prior to 1.2.15. Typical impact of XSS attacks.	6.1	More Details
CVE-2021-31673	A Dom-based Cross-site scripting (XSS) vulnerability at registration account in Cyclos 4 PRO.14.7 and before allows remote attackers to inject arbitrary web script or HTML via the groupId parameter.	6.1	More Details
CVE-2022-29811	In JetBrains Hub before 2022.1.14638 stored XSS via project icon was possible.	6.1	More Details
CVE-2022-29969	The RSS extension before 2022-04-29 for MediaWiki allows XSS via an rss element (if the feed is in $wgRSSUrlWhitelist and $wgRSSAllowLinkTag is true).	6.1	More Details
CVE-2021-31674	Cyclos 4 PRO 4.14.7 and before does not validate user input at error inform, which allows remote unauthenticated attacker to execute javascript code via undefine enum constant.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23617	A cross site scripting (XSS) vulnerability in the error page of Totolink N200RE and N100RE Routers 2.0 allows attackers to execute arbitrary web scripts or HTML via SCRIPT element.	6.1	More Details
CVE-2022-28477	WBCE CMS 1.5.2 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2022-28454	Limbas 4.3.36.1319 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2022-20740	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting attack. This vulnerability is due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by convincing a user to click a link designed to pass malicious input to the interface. A successful exploit could allow the attacker to conduct cross-site scripting attacks and gain access to sensitive browser-based information.	6.1	More Details
CVE-2021-25086	The Advanced Page Visit Counter WordPress plugin before 6.1.2 does not sanitise and escape some input before outputting it in an admin dashboard page, allowing unauthenticated attackers to perform Cross-Site Scripting attacks against admins viewing it	6.1	More Details
CVE-2022-29907	The Nimbus skin for MediaWiki through 1.37.2 (before 6f9c8fb868345701d9544a54d9752515aace39df) allows XSS in Advertise link messages.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1434	The OpenSSL 3.0 implementation of the RC4-MD5 ciphersuite incorrectly uses the AAD data as the MAC key. This makes the MAC key trivially predictable. An attacker could exploit this issue by performing a man-in-the-middle attack to modify data being sent from one endpoint to an OpenSSL 3.0 recipient such that the modified data would still pass the MAC integrity check. Note that data sent from an OpenSSL 3.0 endpoint to a non-OpenSSL 3.0 endpoint will always be rejected by the recipient and the connection will fail at that point. Many application protocols require data to be sent from the client to the server first. Therefore, in such a case, only an OpenSSL 3.0 server would be impacted when talking to a non-OpenSSL 3.0 client. If both endpoints are OpenSSL 3.0 then the attacker could modify data being sent in both directions. In this case both clients and servers could be affected, regardless of the application protocol. Note that in the absence of an attacker this bug means that an OpenSSL 3.0 endpoint communicating with a non-OpenSSL 3.0 endpoint will fail to complete the handshake when using this ciphersuite. The confidentiality of data is not impacted by this issue, i.e. an attacker cannot decrypt data that has been encrypted using this ciphersuite - they can only modify it. In order for this attack to work both endpoints must legitimately negotiate the RC4-MD5 ciphersuite. This ciphersuite is not compiled by default in OpenSSL 3.0, and is not available within the default provider or the default ciphersuite list. This ciphersuite will never be used if TLSv1.3 has been negotiated. In order for an OpenSSL 3.0 endpoint to use this ciphersuite the following must have occurred: 1) OpenSSL must have been compiled with the (non-default) compile time option enable-weak-ssl-ciphers 2) OpenSSL must have had the legacy provider explicitly loaded (either through application code or via configuration) 3) The ciphersuite must have been explicitly added to the ciphersuite list 4) The libssl security level must have been set to 0 (default is 1) 5) A version of SSL/TLS below TLSv1.3 must have been negotiated 6) Both endpoints must negotiate the RC4-MD5 ciphersuite in preference to any others that both endpoints have in common Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2).	5.9	More Details
CVE-2022-28195	NVIDIA Jetson Linux Driver Package contains a vulnerability in the Cboot ext4_read_file function, where insufficient validation of untrusted data may allow a highly privileged local attacker to cause a integer overflow, which may lead to code execution, escalation of privileges, limited denial of service, and some impact to confidentiality and integrity. The scope of impact can extend to other components.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28193	NVIDIA Jetson Linux Driver Package contains a vulnerability in the Cboot module tegrabl_cbo.c, where insufficient validation of untrusted data may allow a local attacker with elevated privileges to cause a memory buffer overflow, which may lead to code execution, loss of integrity, limited denial of service, and some impact to confidentiality.	5.6	More Details
CVE-2022-20101	In aee daemon, there is a possible information disclosure due to a path traversal. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06270870.	5.5	More Details
CVE-2022-20104	In aee daemon, there is a possible information disclosure due to improper access control. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06284104.	5.5	More Details
CVE-2022-29810	The Hashicorp go-getter library before 1.5.11 does not redact an SSH key from a URL query parameter.	5.5	More Details
CVE-2021-42528	XMP Toolkit 2021.07 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-3982	Linux distributions using CAP_SYS_NICE for gnome-shell may be exposed to a privilege escalation issue. An attacker, with low privilege permissions, may take advantage of the way CAP_SYS_NICE is currently implemented and eventually load code to increase its process scheduler priority leading to possible DoS of other services running in the same machine.	5.5	More Details
CVE-2022-1195	A use-after-free vulnerability was found in the Linux kernel in drivers/net/hamradio. This flaw allows a local attacker with a user privilege to cause a denial of service (DOS) when the mkiss or sixpack device is detached and reclaim resources early.	5.5	More Details
CVE-2022-1507	chafa: NULL Pointer Dereference in function gif_internal_decode_frame at libnsgif.c:599 allows attackers to cause a denial of service (crash) via a crafted input file. in GitHub repository hpjansson/chafa prior to 1.10.2. chafa: NULL Pointer Dereference in function gif_internal_decode_frame at libnsgif.c:599 allows attackers to cause a denial of service (crash) via a crafted input file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1515	A memory leak was discovered in matio 1.5.21 and earlier in Mat_VarReadNextInfo5() in mat5.c via a crafted file. This issue can potentially result in DoS.	5.5	More Details
CVE-2022-1475	An integer overflow vulnerability was found in FFmpeg versions before 4.4.2 and before 5.0.1 in g729_parse() in llibavcodec/g729_parser.c when processing a specially crafted file.	5.5	More Details
CVE-2022-1331	In four instances DMARS (All versions prior to v2.1.10.24) does not properly restrict references of XML external entities while processing specific project files, which may allow unauthorized information disclosure.	5.5	More Details
CVE-2022-20092	In alac decoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06366061; Issue ID: ALPS06366061.	5.5	More Details
CVE-2022-21230	This affects all versions of package org.nanohttpd:nanohttpd. Whenever an HTTP Session is parsing the body of an HTTP request, the body of the request is written to a RandomAccessFile when the it is larger than 1024 bytes. This file is created with insecure permissions that allow its contents to be viewed by all users on the host machine. **Workaround:** Manually specifying the -Djava.io.tmpdir= argument when launching Java to set the temporary directory to a directory exclusively controlled by the current user can fix this issue.	5.5	More Details
CVE-2021-38952	IBM InfoSphere Information Server 11.7 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: 211408.	5.4	More Details
CVE-2022-24891	ESAPI (The OWASP Enterprise Security API) is a free, open source, web application security control library. Prior to version 2.3.0.0, there is a potential for a cross-site scripting vulnerability in ESAPI caused by a incorrect regular expression for "onsiteURL" in the **antisamy-esapi.xml** configuration file that can cause "javascript:" URLs to fail to be correctly sanitized. This issue is patched in ESAPI 2.3.0.0. As a workaround, manually edit the **antisamy-esapi.xml** configuration files to change the "onsiteURL" regular expression. More information about remediation of the vulnerability, including the workaround, is available in the maintainers' release notes and security bulletin.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4200	A Improper Privilege Management vulnerability in SUSE Rancher allows write access to the Catalog for any user when restricted-admin role is enabled. This issue affects: SUSE Rancher Rancher versions prior to 2.5.13; Rancher versions prior to 2.6.4.	5.4	More Details
CVE-2021-41948	A cross-site scripting (XSS) vulnerability exists in the "contact us" plugin for Subrion CMS <= 4.2.1 version via "List of subjects".	5.4	More Details
CVE-2022-25349	All versions of package materialize-css are vulnerable to Cross-site Scripting (XSS) due to improper escape of user input (such as <not-a-tag />) that is being parsed as HTML/JavaScript, and inserted into the Document Object Model (DOM). This vulnerability can be exploited when the user-input is provided to the autocomplete component.	5.4	More Details
CVE-2022-21149	The package s-cart/s-cart before 6.9; the package s-cart/core before 6.9 are vulnerable to Cross-site Scripting (XSS) which can lead to cookie stealing of any victim that visits the affected URL so the attacker can gain unauthorized access to that user's account through the stolen cookie.	5.4	More Details
CVE-2022-28102	A cross-site scripting (XSS) vulnerability in PHP MySQL Admin Panel Generator v1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected at /edit-db.php.	5.4	More Details
CVE-2022-24873	Shopware is an open source e-commerce software platform. Prior to version 5.7.9, Shopware is vulnerable to non-stored cross-site scripting in the storefront. This issue is fixed in version 5.7.9. Users of older versions may attempt to mitigate the vulnerability by using the Shopware security plugin.	5.4	More Details
CVE-2022-29414	Multiple (13x) Cross-Site Request Forgery (CSRF) vulnerabilities in WPKube's Subscribe To Comments Reloaded plugin <= 211130 on WordPress allows attackers to clean up Log archive, download system info file, plugin system settings, plugin options settings, generate a new key, reset all options, change notifications settings, management page settings, comment form settings, manage subscriptions > mass update settings, manage subscriptions > add a new subscription, update subscription, delete Subscription.	5.4	More Details
CVE-2022-25854	This affects the package @yaireo/tagify before 4.9.8. The package is used for rendering UI components inside the input or text fields, and an attacker can pass a malicious placeholder value to it to fire the XSS payload.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23065	In Vendure versions 0.1.0-alpha.2 to 1.5.1 are affected by Stored XSS vulnerability, where an attacker having catalog permission can upload a SVG file that contains malicious JavaScript into the “Assets” tab. The uploaded file will affect administrators as well as regular users.	5.4	More Details
CVE-2022-28599	A stored cross-site scripting (XSS) vulnerability exists in FUEL-CMS 1.5.1 that allows an authenticated user to upload a malicious .pdf file which acts as a stored XSS payload. If this stored XSS payload is triggered by an administrator it will trigger a XSS attack.	5.4	More Details
CVE-2022-1514	Stored XSS via upload plugin functionality in zip format in GitHub repository neorazorx/facturascripts prior to 2022.06. Cross-site scripting attacks can have devastating consequences. Code injected into a vulnerable application can exfiltrate data or install malware on the user's machine. Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account.	5.4	More Details
CVE-2021-39390	Stored XSS in PartKeepr 1.4.0 Edit section in multiple api endpoints via name parameter.	5.4	More Details
CVE-2022-29412	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in Hermit 音乐播放器 plugin <= 3.1.6 on WordPress allow attackers to delete cache, delete a source, create source.	5.4	More Details
CVE-2022-28588	In SpringBootMovie <=1.2 when adding movie names, malicious code can be stored because there are no filtering parameters, resulting in stored XSS.	5.4	More Details
CVE-2022-20629	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20628	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	5.4	More Details
CVE-2022-20627	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	5.4	More Details
CVE-2022-29584	Mahara before 20.10.5, 21.04.4, 21.10.2, and 22.04.0 allows stored XSS when a particular Cascading Style Sheets (CSS) class for embedly is used, and JavaScript code is constructed to perform an action.	5.4	More Details
CVE-2022-27330	A cross-site scripting (XSS) vulnerability in /public/admin/index.php?add_product of E-Commerce Website v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Product Title text field.	5.4	More Details
CVE-2022-22443	IBM InfoSphere Information Server 11.7 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: 224440.	5.4	More Details
CVE-2022-22322	IBM InfoSphere Information Server 11.7 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: 218370.	5.4	More Details
CVE-2021-34590	In Bender/ebee Charge Controllers in multiple versions are prone to Cross-site Scripting. An authenticated attacker could write HTML Code into configuration values. These values are not properly escaped when displayed.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22556	The Security Team discovered an integer overflow bug that allows an attacker with code execution to issue memory cache invalidation operations on pages that they don’t own, allowing them to control kernel memory from userspace. We recommend upgrading to kernel version 4.1 or beyond.	5.3	More Details
CVE-2022-1343	The function `OCSP_basic_verify` verifies the signer certificate on an OCSP response. In the case where the (non-default) flag OCSP_NOCHECKS is used then the response will be positive (meaning a successful verification) even in the case where the response signing certificate fails to verify. It is anticipated that most users of `OCSP_basic_verify` will not use the OCSP_NOCHECKS flag. In this case the `OCSP_basic_verify` function will return a negative value (indicating a fatal error) in the case of a certificate verification failure. The normal expected return value in this case would be 0. This issue also impacts the command line OpenSSL "ocsp" application. When verifying an ocsp response with the "-no_cert_checks" option the command line application will report that the verification is successful even though it has in fact failed. In this case the incorrect successful response will also be accompanied by error messages showing the failure and contradicting the apparently successful result. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2).	5.3	More Details
CVE-2022-0882	A bug exists where an attacker can read the kernel log through exposed Zircon kernel addresses without the required capability ZX_RSRC_KIND_ROOT. It is recommended to upgrade the Fuchsia kernel to 4.1.1 or greater.	5.3	More Details
CVE-2021-41041	In Eclipse Openj9 before version 0.32.0, Java 8 & 11 fail to throw the exception captured during bytecode verification when verification is triggered by a MethodHandle invocation, allowing unverified methods to be invoked using MethodHandles.	5.3	More Details
CVE-2022-25844	The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value. **Note:** 1) This package has been deprecated and is no longer maintained. 2) The vulnerable versions are 1.7.0 and higher.	5.3	More Details
CVE-2022-22276	A vulnerability in SonicOS SNMP service resulting exposure of sensitive information to an unauthorized user.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22277	A vulnerability in SonicOS SNMP service resulting exposure of Wireless Access Point sensitive information in cleartext.	5.3	More Details
CVE-2022-29869	cifs-utils through 6.14, with verbose logging, can cause an information leak when a file contains = (equal sign) characters but is not a valid credentials file.	5.3	More Details
CVE-2022-24974	Links may not be rewritten according to policy in some specially formatted emails.	5.3	More Details
CVE-2021-4138	Improved Host header checks to reject requests not sent to a well-known local hostname or IP, or the server-specified hostname.	5.3	More Details
CVE-2021-46423	Telesquare TLR-2005KSH 1.0.0 is affected by an unauthenticated file download vulnerability that allows a remote attacker to download a full configuration file.	5.3	More Details
CVE-2021-38939	IBM QRadar SIEM 7.3, 7.4, and 7.5 stores potentially sensitive information in log files that could be read by an user with access to creating domains. IBM X-Force ID: 211037.	5.3	More Details
CVE-2022-20748	A vulnerability in the local malware analysis process of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the affected device. This vulnerability is due to insufficient error handling in the local malware analysis process of an affected device. An attacker could exploit this vulnerability by sending a crafted file through the device. A successful exploit could allow the attacker to cause the local malware analysis process to crash, which could result in a DoS condition. Notes: Manual intervention may be required to recover from this situation. Malware cloud lookup and dynamic analysis will not be impacted.	5.3	More Details
CVE-2021-34587	In Bender/ebee Charge Controllers in multiple versions a long URL could lead to webserver crash. The URL is used as input of an sprintf to a stack variable.	5.3	More Details
CVE-2021-41810	Admin tool allows storing configuration data with script which may then get run by another vault administrator. Requires vault admin level authentication and is not remotely exploitable	5.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28197	NVIDIA Jetson Linux Driver Package contains a vulnerability in the Cboot ext4_mount function, where Insufficient validation of untrusted data may allow a highly privileged local attacker to cause an integer overflow. This difficult-to-exploit vulnerability may lead to code execution, escalation of privileges, limited denial of service, and some impact to confidentiality and integrity. The scope of impact can extend to other components.	5.0	More Details
CVE-2022-28780	Improper access control vulnerability in Weather prior to SMR May-2022 Release 1 allows that attackers can access location information that set in Weather without permission. The patch adds proper protection to prevent access to location information.	5.0	More Details
CVE-2021-43930	Elcomplus SmartPTT is vulnerable as the backup and restore system does not adequately validate download requests, enabling malicious users to perform path traversal attacks and potentially download arbitrary files from the system.	4.9	More Details
CVE-2022-28117	A Server-Side Request Forgery (SSRF) in feed_parser class of Navigate CMS v2.9.4 allows remote attackers to force the application to make arbitrary requests via injection of arbitrary URLs into the feed parameter.	4.9	More Details
CVE-2022-24898	org.xwiki.commons:xwiki-commons-xml is a common module used by other XWiki top level projects. Starting in version 2.7 and prior to versions 12.10.10, 13.4.4, and 13.8-rc-1, it is possible for a script to access any file accessing to the user running XWiki application server with XML External Entity Injection through the XML script service. The problem has been patched in versions 12.10.10, 13.4.4, and 13.8-rc-1. There is no easy workaround for fixing this vulnerability other than upgrading and being careful when giving Script rights.	4.9	More Details
CVE-2022-0649	The AdRotate WordPress plugin before 5.8.23 does not escape Group Names, 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-2022-23060	A Stored Cross Site Scripting (XSS) vulnerability exists in Shopizer versions 2.0 through 2.17.0, where a privileged user (attacker) can inject malicious JavaScript in the filename under the “Manage files” tab	4.8	More Details
CVE-2022-22345	IBM QRadar 7.3, 7.4, and 7.5 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: 220041.	4.8	More Details
CVE-2022-28589	A stored cross-site scripting (XSS) vulnerability in Pixelimity 1.0 allows attackers to execute arbitrary web scripts or HTML via the Title field in admin/pages.php?action=add_new	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1255	The Import and export users and customers WordPress plugin before 1.19.2.1 does not sanitise and escaped imported CSV data, which could allow high privilege users to import malicious javascript code and lead to Stored Cross-Site Scripting issues	4.8	More Details
CVE-2022-1046	The Visual Form Builder WordPress plugin before 3.0.7 does not sanitise and escape the form's 'Email to' field , 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-2022-0662	The AdRotate WordPress plugin before 5.8.23 does not sanitise and escape Advert Names 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-2022-0418	The Event List WordPress plugin before 0.8.8 does not sanitise and escape some of its settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks against other admin even when the unfiltered_html is disallowed	4.8	More Details
CVE-2021-25102	The All In One WP Security & Firewall WordPress plugin before 4.4.11 does not validate, sanitise and escape the redirect_to parameter before using it to redirect user, either via a Location header, or meta url attribute, when the Rename Login Page is active, which could lead to an Arbitrary Redirect as well as Cross-Site Scripting issue. Exploitation of this issue requires the Login Page URL value to be known, which should be hard to guess, reducing the risk	4.7	More Details
CVE-2022-29973	relan exFAT 1.3.0 allows local users to obtain sensitive information (data from deleted files in the filesystem) in certain situations involving offsets beyond ValidDataLength.	4.7	More Details
CVE-2022-20097	In aee daemon, there is a possible information disclosure due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06383944.	4.7	More Details
CVE-2022-29413	Cross-Site Request Forgery (CSRF) leading to Stored Cross-Site Scripting (XSS) in Mufeng's Hermit 音乐播放器 plugin <= 3.1.6 on WordPress via &title parameter.	4.7	More Details
CVE-2022-24372	Linksys MR9600 devices before 2.0.5 allow attackers to read arbitrary files via a symbolic link to the root directory of a NAS SMB share.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28196	NVIDIA Jetson Linux Driver Package contains a vulnerability in the Cboot blob_decompress function, where insufficient validation of untrusted data may allow a local attacker with elevated privileges to cause a memory buffer overflow, which may lead to code execution, limited loss of Integrity, and limited denial of service. The scope of impact can extend to other components.	4.6	More Details
CVE-2022-28782	Improper access control vulnerability in Contents To Window prior to SMR May-2022 Release 1 allows physical attacker to install package before completion of Setup wizard. The patch blocks entry point of the vulnerability.	4.6	More Details
CVE-2021-27417	eCosCentric eCosPro RTOS Versions 2.0.1 through 4.5.3 are vulnerable to integer wraparound in function calloc (an implementation of malloc). The unverified memory assignment can lead to arbitrary memory allocation, resulting in a heap-based buffer overflow.	4.6	More Details
CVE-2022-20100	In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06270804.	4.4	More Details
CVE-2022-20098	In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06419017; Issue ID: ALPS06419017.	4.4	More Details
CVE-2022-28793	Given the TEE is compromised and controlled by the attacker, improper state maintenance in StrongBox allows attackers to change Android ROT during device boot cycle after compromising TEE. The patch is applied in Galaxy S22 to prevent change of Android ROT after first initialization at boot time.	4.4	More Details
CVE-2022-20729	A vulnerability in CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to inject XML into the command parser. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted input in commands. A successful exploit could allow the attacker to inject XML into the command parser, which could result in unexpected processing of the command and unexpected command output.	4.4	More Details
CVE-2022-20096	In camera, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is no needed for exploitation. Patch ID: ALPS06419003; Issue ID: ALPS06419003.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20102	In aee daemon, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06296442; Issue ID: ALPS06296405.	4.4	More Details
CVE-2022-20103	In aee daemon, there is a possible information disclosure due to symbolic link following. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06383944; Issue ID: ALPS06282684.	4.4	More Details
CVE-2022-20107	In subtitle service, there is a possible application crash due to an integer overflow. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03330673; Issue ID: DTV03330673.	4.4	More Details
CVE-2022-0985	Insufficient capability checks could allow users with the moodle/site:uploadusers capability to delete users, without having the necessary moodle/user:delete capability.	4.3	More Details
CVE-2022-27331	An access control issue in Zammad v5.0.3 broadcasts administrative configuration changes to all users who have an active application instance, including settings that should only be visible to authenticated users.	4.3	More Details
CVE-2022-29903	The Private Domains extension for MediaWiki through 1.37.2 (before 1ad65d4c1c199b375ea80988d99ab51ae068f766) allows CSRF for editing pages that store the extension's configuration. The attacker must trigger a POST request to Special:PrivateDomains.	4.3	More Details
CVE-2021-38874	IBM QRadar SIEM 7.3, 7.4, and 7.5 allows for users to access information across tenant and domain boundaries in some situations. IBM X-Force ID: 208397.	4.3	More Details
CVE-2022-24888	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. Prior to versions 20.0.14.4, 21.0.8, 22.2.4, and 23.0.1, it is possible to create files and folders that have leading and trailing \n, \r, \t, and \v characters. The server rejects files and folders that have these characters in the middle of their names, so this might be an opportunity for injection. This issue is fixed in versions 20.0.14.4, 21.0.8, 22.2.4, and 23.0.1. There are currently no known workarounds.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24887	Nextcloud Talk is a video and audio conferencing app for Nextcloud, a self-hosted productivity platform. Prior to versions 11.3.4, 12.2.2, and 13.0.0, when sharing a Deck card in conversation, the metaData can be manipulated so users can be tricked into opening arbitrary URLs. This issue is fixed in versions 11.3.4, 12.2.2, and 13.0.0. There are currently no known workarounds.	4.3	More Details
CVE-2021-29776	IBM QRadar SIEM 7.3, 7.4, and 7.5 could allow an authenticated user to obtain sensitive information from another user's dashboard providing the dashboard ID of that user. IBM X-Force ID: 203030.	4.3	More Details
CVE-2022-29905	The FanBoxes extension for MediaWiki through 1.37.2 (before 027ffb0b9d6fe0d823810cf03f5b562a212162d4) allows Special:UserBoxes CSRF.	4.3	More Details
CVE-2022-0984	Users with the capability to configure badge criteria (teachers and managers by default) were able to configure course badges with profile field criteria, which should only be available for site badges.	4.3	More Details
CVE-2022-26326	Potential open redirection vulnerability when URL is crafted in specific format in NetIQ Access Manager prior to 5.0.2	4.0	More Details
CVE-2022-28784	Path traversal vulnerability in Galaxy Themes prior to SMR May-2022 Release 1 allows attackers to list file names in arbitrary directory as system user. The patch addresses incorrect implementation of file path validation check logic.	4.0	More Details
CVE-2022-28785	Improper buffer size check logic in aviextractor library prior to SMR May-2022 Release 1 allows out of bounds read leading to possible temporary denial of service. The patch adds buffer size check logic.	4.0	More Details
CVE-2022-28786	Improper buffer size check logic in aviextractor library prior to SMR May-2022 Release 1 allows out of bounds read leading to possible temporary denial of service. The patch adds buffer size check logic.	4.0	More Details
CVE-2022-28787	Improper buffer size check logic in wmfextractor library prior to SMR May-2022 Release 1 allows out of bounds read leading to possible temporary denial of service. The patch adds buffer size check logic.	4.0	More Details
CVE-2022-28788	Improper buffer size check logic in aviextractor library prior to SMR May-2022 Release 1 allows out of bounds read leading to possible temporary denial of service. The patch adds buffer size check logic.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28790	Improper authentication in Link to Windows Service prior to version 2.3.04.1 allows attacker to lock the device. The patch adds proper caller signature check logic.	4.0	More Details
CVE-2022-29945	DJI drone devices sold in 2017 through 2022 broadcast unencrypted information about the drone operator's physical location via the AeroScope protocol.	4.0	More Details
CVE-2022-20730	A vulnerability in the Security Intelligence feed feature of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the Security Intelligence DNS feed. This vulnerability is due to incorrect feed update processing. An attacker could exploit this vulnerability by sending traffic through an affected device that should be blocked by the affected device. A successful exploit could allow the attacker to bypass device controls and successfully send traffic to devices that are expected to be protected by the affected device.	4.0	More Details
CVE-2021-25266	An insecure data storage vulnerability allows a physical attacker with root privileges to retrieve TOTP secret keys from unlocked phones in Sophos Authenticator for Android version 3.4 and older, and Intercept X for Mobile (Android) before version 9.7.3495.	3.9	More Details
CVE-2022-29817	In JetBrains IntelliJ IDEA before 2022.1 reflected XSS via error messages in internal web server was possible	3.9	More Details
CVE-2022-24735	Redis is an in-memory database that persists on disk. By exploiting weaknesses in the Lua script execution environment, an attacker with access to Redis prior to version 7.0.0 or 6.2.7 can inject Lua code that will execute with the (potentially higher) privileges of another Redis user. The Lua script execution environment in Redis provides some measures that prevent a script from creating side effects that persist and can affect the execution of the same, or different script, at a later time. Several weaknesses of these measures have been publicly known for a long time, but they had no security impact as the Redis security model did not endorse the concept of users or privileges. With the introduction of ACLs in Redis 6.0, these weaknesses can be exploited by a less privileged users to inject Lua code that will execute at a later time, when a privileged user executes a Lua script. The problem is fixed in Redis versions 7.0.0 and 6.2.7. An additional workaround to mitigate this problem without patching the redis-server executable, if Lua scripting is not being used, is to block access to `SCRIPT LOAD` and `EVAL` commands using ACL rules.	3.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29818	In JetBrains IntelliJ IDEA before 2022.1 origin checks in the internal web server were flawed	3.9	More Details
CVE-2022-1548	Mattermost Playbooks plugin 1.25 and earlier fails to properly restrict user-level permissions, which allows playbook members to escalate their membership privileges and perform actions restricted to playbook admins.	3.7	More Details
CVE-2022-1503	A vulnerability, which was classified as problematic, has been found in GetSimple CMS. Affected by this issue is the file /admin/edit.php of the Content Module. The manipulation of the argument post-content with an input like <script>alert(1)</script> leads to cross site scripting. The attack may be launched remotely but requires authentication. Expoit details have been disclosed within the advisory.	3.5	More Details
CVE-2022-1526	A vulnerability, which was classified as problematic, was found in Emlog Pro up to 1.2.2. This affects the POST parameter handling of articles. The manipulation with the input <script>alert(1);</script> leads to cross site scripting. It is possible to initiate the attack remotely but it requires a signup and login by the attacker. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-1536	A vulnerability has been found in automad up to 1.10.9 and classified as problematic. This vulnerability affects the Dashboard. The manipulation of the argument title with the input Home</title><script>alert("home") </script><title> leads to a cross site scripting. The attack can be initiated remotely but requires an authentication. The exploit details have disclosed to the public and may be used.	3.5	More Details
CVE-2021-36844	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in MyThemeShop WP Subscribe plugin <= 1.2.12 on WordPress.	3.4	More Details
CVE-2022-24736	Redis is an in-memory database that persists on disk. Prior to versions 6.2.7 and 7.0.0, an attacker attempting to load a specially crafted Lua script can cause NULL pointer dereference which will result with a crash of the redis-server process. The problem is fixed in Redis versions 7.0.0 and 6.2.7. An additional workaround to mitigate this problem without patching the redis-server executable, if Lua scripting is not being used, is to block access to `SCRIPT LOAD` and `EVAL` commands using ACL rules.	3.3	More Details
CVE-2022-1249	A NULL pointer dereference flaw was found in pesign's cms_set_pw_data() function of the cms_common.c file. The function fails to handle the NULL pwdata invocation from daemon.c, which leads to an explicit NULL dereference and crash on all attempts to daemonize pesign.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29820	In JetBrains PyCharm before 2022.1 exposure of the debugger port to the internal network was possible	3.0	More Details
CVE-2022-26325	Reflected Cross Site Scripting (XSS) vulnerability in NetIQ Access Manager prior to 5.0.2	2.9	More Details
CVE-2022-29816	In JetBrains IntelliJ IDEA before 2022.1 HTML injection into IDE messages was possible	2.8	More Details
CVE-2022-24889	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. Prior to versions 21.0.8, 22.2.4, and 23.0.1, it is possible to trick administrators into enabling "recommended" apps for the Nextcloud server that they do not need, thus expanding their attack surface unnecessarily. This issue is fixed in versions 21.0.8 , 22.2.4, and 23.0.1.	2.4	More Details
CVE-2022-29812	In JetBrains IntelliJ IDEA before 2022.1 notification mechanisms about using Unicode directionality formatting characters were insufficient	2.3	More Details
CVE-2022-24886	Nextcloud Android app is the Android client for Nextcloud, a self-hosted productivity platform. In versions prior to 3.19.0, any application with notification permission can access contacts if Nextcloud has access to Contacts without applying for the Contacts permission itself. Version 3.19.0 contains a fix for this issue. There are currently no known workarounds.	2.2	More Details
CVE-2022-24885	Nextcloud Android app is the Android client for Nextcloud, a self-hosted productivity platform. Prior to version 3.19.1, users can bypass a lock on the Nextcloud app on an Android device by repeatedly reopening the app. Version 3.19.1 contains a fix for the problem. There are currently no known workarounds.	2.0	More Details
CVE-2021-32500	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2022-1214	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This CVE has been rejected as it was incorrectly assigned. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details