SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 08 June 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-31481	An unauthenticated attacker can send a specially crafted update file to the device that can overflow a buffer. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.302 for the LP series and 1.296 for the EP series. The overflowed data can allow the attacker to manipulate the “normal” code execution to that of their choosing. An attacker with this level of access on the device can monitor all communications sent to and from this device, modify onboard relays, change configuration files, or cause the device to become unstable.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1680	An account takeover issue has been discovered in GitLab EE affecting all versions starting from 11.10 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting from 15.0 before 15.0.1. When group SAML SSO is configured, the SCIM feature (available only on Premium+ subscriptions) may allow any owner of a Premium group to invite arbitrary users through their username and email, then change those users' email addresses via SCIM to an attacker controlled email address and thus - in the absence of 2FA - take over those accounts. It is also possible for the attacker to change the display name and username of the targeted account.	9.9	More Details
CVE-2022-29875	A vulnerability has been identified in Biograph Horizon PET/CT Systems (All VJ30 versions < VJ30C-UD01), MAGNETOM Family (NUMARIS X: VA12M, VA12S, VA10B, VA20A, VA30A, VA31A), MAMMOMAT Revelation (All VC20 versions < VC20D), NAEOTOM Alpha (All VA40 versions < VA40 SP2), SOMATOM X.cite (All versions < VA30 SP5 or VA40 SP2), SOMATOM X.creed (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.All (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Now (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Open Pro (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Sim (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Top (All versions < VA30 SP5 or VA40 SP2), SOMATOM go.Up (All versions < VA30 SP5 or VA40 SP2), Symbia E/S (All VB22 versions < VB22A-UD03), Symbia Evo (All VB22 versions < VB22A-UD03), Symbia Intevo (All VB22 versions < VB22A-UD03), Symbia T (All VB22 versions < VB22A-UD03), Symbia.net (All VB22 versions < VB22A-UD03), syngo.via VB10 (All versions), syngo.via VB20 (All versions), syngo.via VB30 (All versions), syngo.via VB40 (All versions < VB40B HF06), syngo.via VB50 (All versions), syngo.via VB60 (All versions < VB60B HF02). The application deserialises untrusted data without sufficient validations that could result in an arbitrary deserialization. This could allow an unauthenticated attacker to execute code in the affected system if ports 32912/tcp or 32914/tcp are reachable.	9.8	More Details
CVE-2022-31951	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/classes/Master.php?f=delete_respondent_type.	9.8	More Details
CVE-2022-31976	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/classes/Master.php?f=delete_request.	9.8	More Details
CVE-2022-31969	ChatBot App with Suggestion v1.0 is vulnerable to SQL Injection via /simple_chat_bot/admin/?page=user/manage_user&id=.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31965	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/admin/respondent_types/manage_respondent_type.php?id=.	9.8	More Details
CVE-2022-31964	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via rdms/admin/respondent_types/view_respondent_type.php?id=.	9.8	More Details
CVE-2022-31962	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/admin/incidents/view_incident.php?id=.	9.8	More Details
CVE-2022-31961	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/admin/incidents/manage_incident.php?id=.	9.8	More Details
CVE-2022-31959	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/admin/teams/manage_team.php?id=.	9.8	More Details
CVE-2022-31957	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via rdms/admin/teams/view_team.php?id=.	9.8	More Details
CVE-2022-31956	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/admin/incident_reports/manage_report.php?id=.	9.8	More Details
CVE-2022-31953	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/admin/incident_reports/view_report.php?id=.	9.8	More Details
CVE-2022-31952	Rescue Dispatch Management System v1.0 is vulnerable to SQL injection via /rdms/classes/Master.php?f=delete_incident.	9.8	More Details
CVE-2022-31946	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/classes/Master.php?f=delete_team.	9.8	More Details
CVE-2022-31948	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via /rdms/classes/Master.php?f=delete_report.	9.8	More Details
CVE-2022-31978	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/classes/Master.php?f=delete_inquiry.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31799	Bottle before 0.12.20 mishandles errors during early request binding.	9.8	More Details
CVE-2022-31354	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/classes/Master.php?f=get_vehicle_service.	9.8	More Details
CVE-2022-31353	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/admin/services/view_service.php?id=.	9.8	More Details
CVE-2022-31352	Online Car Wash Booking System v1.0 by oretnom23 has SQL injection in /ocwbs/admin/services/manage_service.php?id=.	9.8	More Details
CVE-2022-31351	Online Car Wash Booking System v1.0 by oretnom23 has SQL injection via /ocwbs/admin/services/manage_price.php?id=.	9.8	More Details
CVE-2022-31350	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/admin/vehicles/manage_vehicle.php?id=.	9.8	More Details
CVE-2022-31348	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/admin/bookings/update_status.php?id=.	9.8	More Details
CVE-2022-31347	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/classes/Master.php?f=delete_vehicle.	9.8	More Details
CVE-2019-12349	An issue was discovered in zzcms 2019. SQL Injection exists in /admin/dl_sendsms.php via the id parameter.	9.8	More Details
CVE-2022-31345	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/admin/?page=user/manage_user&id=.	9.8	More Details
CVE-2022-31977	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/classes/Master.php?f=delete_team.	9.8	More Details
CVE-2022-32002	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/courts/manage_court.php?id=.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31343	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/admin/?page=bookings/view_details&id=.	9.8	More Details
CVE-2022-31989	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page=user/manage_user&id=.	9.8	More Details
CVE-2022-30927	A SQL injection vulnerability exists in Simple Task Scheduling System 1.0 when MySQL is being used as the application database. An attacker can issue SQL commands to the MySQL database through the vulnerable "id" parameter.	9.8	More Details
CVE-2022-32511	jmespath.rb (aka JMESPath for Ruby) before 1.6.1 uses JSON.load in a situation where JSON.parse is preferable.	9.8	More Details
CVE-2022-31768	IBM InfoSphere Information Server 11.7 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database.	9.8	More Details
CVE-2022-26134	In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. The affected versions are from 1.3.0 before 7.4.17, from 7.13.0 before 7.13.7, from 7.14.0 before 7.14.3, from 7.15.0 before 7.15.2, from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and from 7.18.0 before 7.18.1.	9.8	More Details
CVE-2022-26493	Xecurify's miniOrange Premium, Standard, and Enterprise Drupal SAML SP modules possess an authentication and authorization bypass vulnerability. An attacker with access to a HTTP-request intercepting method is able to bypass authentication and authorization by removing the SAML Assertion Signature - impersonating existing users and existing roles, including administrative users/roles. This vulnerability is not mitigated by configuring the module to enforce signatures or certificate checks. Xecurify recommends updating miniOrange modules to their most recent versions. This vulnerability is present in paid versions of the miniOrange Drupal SAML SP product affecting Drupal 7, 8, and 9.	9.8	More Details
CVE-2021-42890	TOTOLINK EX1200T V4.1.2cu.5215 contains a remote command injection vulnerability in function NTPSyncWithHost of the file system.so which can control hostTime to attack.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42888	TOTOLINK EX1200T V4.1.2cu.5215 contains a remote command injection vulnerability in function setLanguageCfg of the file global.so which can control langType to attack.	9.8	More Details
CVE-2021-42887	In TOTOLINK EX1200T V4.1.2cu.5215, an attacker can bypass login by sending a specific request through formLoginAuth.htm.	9.8	More Details
CVE-2021-42885	TOTOLINK EX1200T V4.1.2cu.5215 contains a remote command injection vulnerability in function setDeviceMac of the file global.so which can control deviceName to attack.	9.8	More Details
CVE-2021-42884	TOTOLINK EX1200T V4.1.2cu.5215 contains a remote command injection vulnerability in function setDeviceName of the file global.so which can control thedeviceName to attack.	9.8	More Details
CVE-2022-32270	In Real Player 20.0.7.309 and 20.0.8.310, external::Import() allows download of arbitrary file types and Directory Traversal, leading to Remote Code Execution. This occurs because it is possible to plant executables in the startup folder (DLL planting could also occur).	9.8	More Details
CVE-2022-32269	In Real Player 20.0.8.310, the G2 Control allows injection of unsafe javascript: URIs in local HTTP error pages (displayed by Internet Explorer core). This leads to arbitrary code execution.	9.8	More Details
CVE-2022-26869	Dell PowerStore versions 2.0.0.x, 2.0.1.x and 2.1.0.x contains an open port vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to information disclosure and arbitrary code execution.	9.8	More Details
CVE-2021-42875	TOTOLINK EX1200T V4.1.2cu.5215 contains a remote command injection vulnerability in the function setDiagnosisCfg of the file lib/cste_modules/system.so to control the ipDoamin.	9.8	More Details
CVE-2022-32019	Car Rental Management System v1.0 is vulnerable to Arbitrary code execution via car-rental-management-system/admin/ajax.php?action=save_car.	9.8	More Details
CVE-2022-29704	BrowsBox CMS v4.0 was discovered to contain a SQL injection vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25163	Improper Input Validation vulnerability in Mitsubishi Electric MELSEC-Q Series QJ71E71-100 first 5 digits of serial number "24061" or prior, Mitsubishi Electric MELSEC-L series LJ71E71-100 first 5 digits of serial number "24061" or prior and Mitsubishi Electric MELSEC iQ-R Series RD81MES96N firmware version "08" or prior allows a remote unauthenticated attacker to cause a denial of service (DoS) condition or execute malicious code on the target products by sending specially crafted packets.	9.8	More Details
CVE-2021-45983	NetScout nGeniusONE 6.3.2 allows Java RMI Code Execution.	9.8	More Details
CVE-2021-45981	NetScout nGeniusONE 6.3.2 allows an XML External Entity (XXE) attack.	9.8	More Details
CVE-2022-32020	Car Rental Management System v1.0 is vulnerable to Arbitrary code execution via ip/car-rental-management-system/admin/ajax.php?action=save_settings.	9.8	More Details
CVE-2022-31993	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/classes/Master.php?f=delete_service.	9.8	More Details
CVE-2022-31991	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/classes/Master.php?f=delete_court.	9.8	More Details
CVE-2022-31990	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/classes/Master.php?f=delete_product.	9.8	More Details
CVE-2022-31344	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/classes/Master.php?f=delete_booking.	9.8	More Details
CVE-2022-31346	Online Car Wash Booking System v1.0 is vulnerable to SQL Injection via /ocwbs/classes/Master.php?f=delete_service.	9.8	More Details
CVE-2022-31340	Simple Inventory System v1.0 is vulnerable to SQL Injection via /inventory/table_edit_ajax.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30352	phpABook 0.9i is vulnerable to SQL Injection due to insufficient sanitization of user-supplied data in the "auth_user" parameter in index.php script.	9.8	More Details
CVE-2022-29777	Onlyoffice Document Server v6.0.0 and below and Core 6.1.0.26 and below were discovered to contain a heap overflow via the component DesktopEditor/fontengine/fontconverter/FontFileBase.h.	9.8	More Details
CVE-2022-31338	Online Ordering System 2.3.2 is vulnerable to SQL Injection via /ordering/admin/user/index.php?view=edit&id=.	9.8	More Details
CVE-2022-29730	USR IOT 4G LTE Industrial Cellular VPN Router v1.0.36 was discovered to contain hard-coded credentials for its highest privileged account. The credentials cannot be altered through normal operation of the device.	9.8	More Details
CVE-2022-29712	LibreNMS v22.3.0 was discovered to contain multiple command injection vulnerabilities via the service_ip, hostname, and service_param parameters.	9.8	More Details
CVE-2022-29659	Responsive Online Blog v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at single.php.	9.8	More Details
CVE-2022-28945	An issue in Webbank WeCube v3.2.2 allows attackers to execute a directory traversal via a crafted ZIP file.	9.8	More Details
CVE-2022-28605	Hardcoded admin token in SoundBar apps in Linkplay SDK 1.00 allows remote attackers to gain admin privilege access in linkplay antifactory	9.8	More Details
CVE-2022-25237	Bonita Web 2021.2 is affected by a authentication/authorization bypass vulnerability due to an overly broad exclude pattern used in the RestAPIAuthorizationFilter. By appending ;i18ntranslation or /../i18ntranslation/ to the end of a URL, users with no privileges can access privileged API endpoints. This can lead to remote code execution by abusing the privileged API actions.	9.8	More Details
CVE-2022-24702	An issue was discovered in WinAPRS 2.9.0. A buffer overflow in the VHF KISS TNC component allows a remote attacker to achieve remote code execution via malicious AX.25 packets over the air. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24240	ACEweb Online Portal 3.5.065 was discovered to contain a SQL injection vulnerability via the criteria parameter in showschedule.awp.	9.8	More Details
CVE-2022-24239	ACEweb Online Portal 3.5.065 was discovered to contain an unrestricted file upload vulnerability via attachments.awp.	9.8	More Details
CVE-2022-1660	The affected products are vulnerable of untrusted data due to deserialization without prior authorization/authentication, which may allow an attacker to remotely execute arbitrary code.	9.8	More Details
CVE-2021-44098	EGavilan Media Expense-Management-System 1.0 is vulnerable to SQL Injection via /expense_action.php. This allows a remote attacker to compromise Application SQL database.	9.8	More Details
CVE-2021-44097	EGavilan Media Contact-Form-With-Messages-Entry-Management 1.0 is vulnerable to SQL Injection via Addmessage.php. This allows a remote attacker to compromise Application SQL database.	9.8	More Details
CVE-2021-44096	EGavilan Media User-Registration-and-Login-System-With-Admin-Panel 1.0 is vulnerable to SQL Injection via profile_action - update_user. This allows a remote attacker to compromise Application SQL database.	9.8	More Details
CVE-2021-44095	A SQL injection vulnerability exists in ProjectWorlds Hospital Management System in php 1.0 on login page that allows a remote attacker to compromise Application SQL database.	9.8	More Details
CVE-2021-42872	TOTOLINK EX1200T V4.1.2cu.5215 is affected by a command injection vulnerability that can remotely execute arbitrary code.	9.8	More Details
CVE-2021-34084	OS command injection vulnerability in Turistforeningen node-s3-uploader through 2.0.3 for Node.js allows attackers to execute arbitrary commands via the metadata() function.	9.8	More Details
CVE-2021-34082	OS Command Injection vulnerability in allenhwkim proctree through 0.1.1 and commit 0ac10ae575459457838f14e21d5996f2fa5c7593 for Node.js, allows attackers to execute arbitrary commands via the fix function.	9.8	More Details
CVE-2021-34080	OS Command Injection vulnerability in es128 ssl-utils 1.0.0 for Node.js allows attackers to execute arbitrary commands via unsanitized shell metacharacters provided to the createCertRequest() and the createCert() functions.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34079	OS Command injection vulnerability in Mintzo Docker-Tester through 1.2.1 allows attackers to execute arbitrary commands via shell metacharacters in the 'ports' entry of a crafted docker-compose.yml file.	9.8	More Details
CVE-2021-26634	SQL injection and file upload attacks are possible due to insufficient validation of input values in some parameters and variables of files compromising Maxboard, which may lead to arbitrary code execution or privilege escalation. Attackers can use these vulnerabilities to perform attacks such as stealing server management rights using a web shell.	9.8	More Details
CVE-2020-28246	A Server-Side Template Injection (SSTI) was discovered in Form.io 2.0.0. This leads to Remote Code Execution during deletion of the default Email template URL. NOTE: the email templating service was removed after 2020. Additionally, the vendor disputes this issue indicating this is sandboxed and only executable by admins.	9.8	More Details
CVE-2019-12351	An issue was discovered in zzcms 2019. SQL Injection exists in dl/dl_print.php via an id parameter value with a trailing comma.	9.8	More Details
CVE-2019-12350	An issue was discovered in zzcms 2019. SQL Injection exists in dl/dl_download.php via an id parameter value with a trailing comma.	9.8	More Details
CVE-2022-30324	HashiCorp Nomad and Nomad Enterprise version 0.2.0 up to 1.3.0 were impacted by go-getter vulnerabilities enabling privilege escalation through the artifact stanza in submitted jobs onto the client agent host. Fixed in 1.1.14, 1.2.8, and 1.3.1.	9.8	More Details
CVE-2022-29776	Onlyoffice Document Server v6.0.0 and below and Core 6.1.0.26 and below were discovered to contain a stack overflow via the component DesktopEditor/common/File.cpp.	9.8	More Details
CVE-2022-30423	Merchandise Online Store v1.0 by oretnom23 has an arbitrary code execution (RCE) vulnerability in the user profile upload point in the system information.	9.8	More Details
CVE-2022-30809	elitecms 1.01 is vulnerable to SQL Injection via /admin/edit_page.php?page=.	9.8	More Details
CVE-2022-31337	Online Ordering System 2.3.2 is vulnerable to SQL Injection via /ordering/admin/category/index.php?view=edit&id=.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31336	Online Ordering System 2.3.2 is vulnerable to SQL Injection via /ordering/admin/stockin/loaddata.php.	9.8	More Details
CVE-2022-31335	Online Ordering System 2.3.2 is vulnerable to SQL Injection via /ordering/admin/stockin/index.php?view=edit&id=.	9.8	More Details
CVE-2022-31329	Online Ordering System By janobe 2.3.2 is vulnerable to SQL Injection via /ordering/admin/orders/loaddata.php.	9.8	More Details
CVE-2022-31328	Online Ordering System By janobe 2.3.2 has SQL Injection via /ordering/admin/products/index.php?view=edit&id=.	9.8	More Details
CVE-2022-31327	Online Ordering System By janobe 2.3.2 is vulneranle to SQL Injection via /ordering/index.php?q=products&id=.	9.8	More Details
CVE-2022-30817	Simple Bus Ticket Booking System 1.0 is vulnerable to SQL Injection via /SimpleBusTicket/index.php.	9.8	More Details
CVE-2022-30816	elitecms 1.01 is vulnerable to SQL Injection via /admin/edit_sidebar.php.	9.8	More Details
CVE-2022-30815	elitecms 1.01 is vulnerable to SQL Injection via admin/edit_sidebar.php?page=2&sidebar=	9.8	More Details
CVE-2022-30814	elitecms v1.01 is vulnerable to SQL Injection via /admin/add_sidebar.php.	9.8	More Details
CVE-2022-30813	elitecms 1.01 is vulnerable to SQL Injection via /admin/add_post.php.	9.8	More Details
CVE-2022-30470	In Afian Filerun 20220202 Changing the "search_tika_path" variable to a custom (and previously uploaded) jar file results in remote code execution in the context of the webserver user.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30810	elitecms v1.01 is vulnerable to SQL Injection via admin/edit_post.php.	9.8	More Details
CVE-2022-30511	School Dormitory Management System 1.0 is vulnerable to SQL Injection via accounts/view_details.php:4.	9.8	More Details
CVE-2022-30506	An arbitrary file upload vulnerability was discovered in MCMS 5.2.7, allowing an attacker to execute arbitrary code through a crafted ZIP file.	9.8	More Details
CVE-2022-30808	elitecms 1.0.1 is vulnerable to Arbitrary code execution via admin/manage_uploads.php.	9.8	More Details
CVE-2022-30478	Ecommerce-project-with-php-and-mysqli-Fruits-Bazar 1.0 is vulnerable to SQL Injection in \search_product.php via the keyword parameters.	9.8	More Details
CVE-2022-30481	Food-order-and-table-reservation-system- 1.0 is vulnerable to SQL Injection in categorywise-menu.php via the catid parameters.	9.8	More Details
CVE-2022-30797	Online Ordering System 1.0 by oretnom23 is vulnerable to SQL Injection via admin/vieworders.php.	9.8	More Details
CVE-2022-30521	The LAN-side Web-Configuration Interface has Stack-based Buffer Overflow vulnerability in the D-Link Wi-Fi router firmware DIR-890L DIR890LA1_FW107b09.bin and previous versions. The function created at 0x17958 of /htdocs/cgibin will call sprintf without checking the length of strings in parameters given by HTTP header and can be controlled by users easily. The attackers can exploit the vulnerability to carry out arbitrary code by means of sending a specially constructed payload to port 49152.	9.8	More Details
CVE-2022-30512	School Dormitory Management System 1.0 is vulnerable to SQL Injection via accounts/payment_history.php:31.	9.8	More Details
CVE-2022-30490	Badminton Center Management System V1.0 is vulnerable to SQL Injection via parameter 'id' in /bcms/admin/court_rentals/update_status.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30510	School Dormitory Management System 1.0 is vulnerable to SQL Injection via reports/daily_collection_report.php:59.	9.8	More Details
CVE-2022-32271	In Real Player 20.0.8.310, there is a DCP:// URI Remote Arbitrary Code Execution Vulnerability. This is an internal URL Protocol used by Real Player to reference a file that contains an URL. It is possible to inject script code to arbitrary domains. It is also possible to reference arbitrary local files.	9.6	More Details
CVE-2022-31479	An unauthenticated attacker can update the hostname with a specially crafted name that will allow for shell commands to be executed during the core collection process. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.302 for the LP series and 1.296 for the EP series. An attacker with this level of access on the device can monitor all communications sent to and from this device, modify onboard relays, change configuration files, or cause the device to become unstable. The injected commands only get executed during start up or when unsafe calls regarding the hostname are used. This allows the attacker to gain remote access to the device and can make their persistence permanent by modifying the filesystem.	9.6	More Details
CVE-2022-30234	A CWE-798: Use of Hard-coded Credentials vulnerability exists that could allow arbitrary code to be executed when root level access is obtained. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior)	9.4	More Details
CVE-2022-31462	Owl Labs Meeting Owl 5.2.0.15 allows attackers to control the device via a backdoor password (derived from the serial number) that can be found in Bluetooth broadcast data.	9.3	More Details
CVE-2022-31483	An authenticated attacker can upload a file with a filename including “..” and “/” to achieve the ability to upload the desired file anywhere on the filesystem. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.271. This allows a malicious actor to overwrite sensitive system files and install a startup service to gain remote access to the underlaying Linux operating system with root privileges.	9.1	More Details
CVE-2022-31945	Rescue Dispatch Management System v1.0 is vulnerable to Delete any file via /rdms/classes/Master.php?f=delete_img.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33473	An argument injection vulnerability in Dragonfly Ruby Gem v1.3.0 allows attackers to read and write arbitrary files when the verify_url option is disabled. This vulnerability is exploited via a crafted URL.	9.1	More Details
CVE-2022-25361	WatchGuard Firebox and XTM appliances allow an unauthenticated remote attacker to delete arbitrary files from a limited set of directories on the system. This vulnerability impacts Fireware OS before 12.7.2_U2, 12.x before 12.1.3_U8, and 12.2.x through 12.5.x before 12.5.9_U2.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-34081	OS Command Injection vulnerability in bbultman gitsome through 0.2.3 allows attackers to execute arbitrary commands via a crafted tag name of the target git repository.	8.8	More Details
CVE-2022-31486	An authenticated attacker can send a specially crafted route to the “edit_route.cgi” binary and have it execute shell commands. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.303 for the LP series and 1.297 for the EP series. An attacker with this level of access on the device can monitor all communications sent to and from this device, modify onboard relays, change configuration files, or cause the device to become unstable.	8.8	More Details
CVE-2021-32546	Missing input validation in internal/db/repo_editor.go in Gogs before 0.12.8 allows an attacker to execute code remotely. An unprivileged attacker (registered user) can overwrite the Git configuration in his repository. This leads to Remote Command Execution, because that configuration can contain an option such as sshCommand, which is executed when a master branch is a remote branch (using an ssh:// URI). The remote branch can also be configured by editing the Git configuration file. One can create a new file in a new repository, using the GUI, with "\" as its name, and then rename this file to .git/config with the custom configuration content (and then save it).	8.8	More Details
CVE-2022-30822	In Wedding Management System v1.0, there is an arbitrary file upload vulnerability in the picture upload point of "users_profile.php" file.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34078	lifion-verify-dependencies through 1.1.0 is vulnerable to OS command injection via a crafted dependency name on the scanned project's package.json file.	8.8	More Details
CVE-2022-29778	D-Link DIR-890L 1.20b01 allows attackers to execute arbitrary code due to the hardcoded option Wake-On-Lan for the parameter 'descriptor' at SetVirtualServerSettings.php	8.8	More Details
CVE-2021-45982	NetScout nGeniusONE 6.3.2 allows Arbitrary File Upload by a privileged user.	8.8	More Details
CVE-2019-9971	PhoneSystem Terminal in 3CX Phone System (Debian based installation) 16.0.0.1570 allows an attacker to gain root privileges by using sudo with the tcpdump command, without a password. This occurs because the -z (aka postrotate-command) option to tcpdump can be unsafe when used in conjunction with sudo.	8.8	More Details
CVE-2019-9972	PhoneSystem Terminal in 3CX Phone System (Debian based installation) 16.0.0.1570 allows an authenticated attacker to run arbitrary commands with the phonesystem user privileges because of "<space><space> followed by <shift><enter>" mishandling.	8.8	More Details
CVE-2020-36529	A vulnerability classified as critical has been found in SevOne Network Management System up to 5.7.2.22. This affects the file traceroute.php of the Traceroute Handler. The manipulation leads to privilege escalation with a command injection. It is possible to initiate the attack remotely.	8.8	More Details
CVE-2022-30821	In Wedding Management System v1.0, the editing function of the "Services" module in the background management system has an arbitrary file upload vulnerability in the picture upload point of "package_edit.php" file.	8.8	More Details
CVE-2022-29725	An arbitrary file upload in the image upload component of wityCMS v0.6.2 allows attackers to execute arbitrary code via a crafted PHP file.	8.8	More Details
CVE-2022-30820	In Wedding Management v1.0, there is an arbitrary file upload vulnerability in the picture upload point of "users_edit.php" file.	8.8	More Details
CVE-2022-30819	In Wedding Management System v1.0, there is an arbitrary file upload vulnerability in the picture upload point of "photos_edit.php" file.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28799	The TikTok application before 23.7.3 for Android allows account takeover. A crafted URL (unvalidated deeplink) can force the com.zhiliaoapp.musically WebView to load an arbitrary website. This may allow an attacker to leverage an attached JavaScript interface for the takeover with one click.	8.8	More Details
CVE-2021-41932	A blind SQL injection vulnerability in search form in TeamMate+ Audit version 28.0.19.0 allows any authenticated user to create malicious SQL injections, which can result in complete database compromise, gaining information about other users, unauthorized access to audit data etc.	8.8	More Details
CVE-2022-29735	Delta Controls enteliTOUCH 3.40.3935, 3.40.3706, and 3.33.4005 allows attackers to execute arbitrary commands via a crafted HTTP request.	8.8	More Details
CVE-2022-22767	Specific BD Pyxis™ products were installed with default credentials and may presently still operate with these credentials. There may be scenarios where BD Pyxis™ products are installed with the same default local operating system credentials or domain-joined server(s) credentials that may be shared across product types. If exploited, threat actors may be able to gain privileged access to the underlying file system and could potentially exploit or gain access to ePHI or other sensitive information.	8.8	More Details
CVE-2022-30425	Tenda Technology Co.,Ltd HG6 3.3.0-210926 was discovered to contain a command injection vulnerability via the pingAddr and traceAddr parameters. This vulnerability is exploited via a crafted POST request.	8.8	More Details
CVE-2022-29647	An issue was discovered in MCMS 5.2.7. There is a CSRF vulnerability that can add an administrator account via ms/basic/manager/save.do.	8.8	More Details
CVE-2022-32291	In Real Player through 20.1.0.312, attackers can execute arbitrary code by placing a UNC share pathname (for a DLL file) in a RAM file.	8.8	More Details
CVE-2020-20971	Cross Site Request Forgery (CSRF) vulnerability in PbootCMS v2.0.3 via /admin.php?p=/User/index.	8.8	More Details
CVE-2022-21745	In WIFI Firmware, there is a possible memory corruption due to a use after free. This could lead to remote escalation of privilege, when devices are connecting to the attacker-controllable Wi-Fi hotspot, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468872; Issue ID: ALPS06468872.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24848	DHIS2 is an information system for data capture, management, validation, analytics and visualization. A SQL injection security vulnerability affects the `/api/programs/orgUnits?programs=` API endpoint in DHIS2 versions prior to 2.36.10.1 and 2.37.6.1. The system is vulnerable to attack only from users that are logged in to DHIS2, and there is no known way of exploiting the vulnerability without first being logged in as a DHIS2 user. The vulnerability is not exposed to a non-malicious user and requires a conscious attack to be exploited. A successful exploit of this vulnerability could allow the malicious user to read, edit and delete data in the DHIS2 instance's database. Security patches are now available for DHIS2 versions 2.36.10.1 and 2.37.6.1. One may apply mitigations at the web proxy level as a workaround. More information about these mitigations is available in the GitHub Security Advisory.	8.8	More Details
CVE-2022-29624	An arbitrary file upload vulnerability in the Add File function of TPCMS v3.2 allows attackers to execute arbitrary code via a crafted PHP file.	8.8	More Details
CVE-2022-32268	StarWind SAN and NAS v0.2 build 1914 allow remote code execution. A flaw was found in REST API in StarWind Stack. REST command, which allows changing the hostname, doesn’t check a new hostname parameter. It goes directly to bash as part of a script. An attacker with non-root user access can inject arbitrary data into the command that will be executed with root privileges.	8.8	More Details
CVE-2022-30469	In Afian Filerun 20220202, lack of sanitization of the POST parameter "metadata[]" in `/?module=fileman&section=get&page=grid` leads to SQL injection.	8.8	More Details
CVE-2022-30999	FriendsofFlarum (FoF) Upload is an extension that handles file uploads intelligently for your forum. If FoF Upload prior to version 1.2.3 is configured to allow the uploading of SVG files ('image/svg+xml'), navigating directly to an SVG file URI could execute arbitrary Javascript code decided by an attacker. This Javascript code could include the execution of HTTP web requests to Flarum, or any other web service. This could allow data to be leaked by an authenticated Flarum user, or, possibly, for data to be modified maliciously. This issue has been patched with v1.2.3, which now sanitizes uploaded SVG files. As a workaround, remove the ability for users to upload SVG files through FoF Upload.	8.7	More Details
CVE-2022-30235	A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could allow unauthorized access when an attacker uses brute force. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior)	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30034	Flower, a web UI for the Celery Python RPC framework, all versions as of 05-02-2022 is vulnerable to an OAuth authentication bypass. An attacker could then access the Flower API to discover and invoke arbitrary Celery RPC calls or deny service by shutting down Celery task nodes.	8.6	More Details
CVE-2022-30711	Improper validation vulnerability in FeedsInfo prior to SMR Jun-2022 Release 1 allows attackers to launch certain activities.	8.5	More Details
CVE-2022-30712	Improper validation vulnerability in KfaOptions prior to SMR Jun-2022 Release 1 allows attackers to launch certain activities.	8.5	More Details
CVE-2022-30710	Improper validation vulnerability in RemoteViews prior to SMR Jun-2022 Release 1 allows attackers to launch certain activities.	8.5	More Details
CVE-2022-30713	Improper validation vulnerability in LSOItemData prior to SMR Jun-2022 Release 1 allows attackers to launch certain activities.	8.5	More Details
CVE-2022-30238	A CWE-287: Improper Authentication vulnerability exists that could allow an attacker to take over the admin account when an attacker hijacks a session. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior)	8.3	More Details
CVE-2022-30128	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-30127	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details
CVE-2022-31463	Owl Labs Meeting Owl 5.2.0.15 does not require a password for Bluetooth commands, because only client-side authentication is used.	8.2	More Details
CVE-2022-30236	A CWE-669: Incorrect Resource Transfer Between Spheres vulnerability exists that could allow unauthorized access when an attacker uses cross-domain attacks. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior)	8.2	More Details
CVE-2022-30237	A CWE-311: Missing Encryption of Sensitive Data vulnerability exists that could allow authentication credentials to be recovered when an attacker breaks the encoding. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior)	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29084	Dell Unity, Dell UnityVSA, and Dell Unity XT versions before 5.2.0.0.5.173 do not restrict excessive authentication attempts in Unisphere GUI. A remote unauthenticated attacker may potentially exploit this vulnerability to brute-force passwords and gain access to the system as the victim. Account takeover is possible if weak passwords are used by users.	8.1	More Details
CVE-2022-27778	A use of incorrectly resolved name vulnerability fixed in 7.83.1 might remove the wrong file when `--no-clobber` is used together with `--remove-on-error`.	8.1	More Details
CVE-2022-29098	Dell PowerScale OneFS versions 8.2.0.x through 9.3.0.x, contain a weak password requirement vulnerability. An administrator may create an account with no password. A remote attacker may potentially exploit this leading to a user account compromise.	8.1	More Details
CVE-2022-27438	Caphyon Ltd Advanced Installer 19.3 and earlier and many products that use the updater from Advanced Installer (Advanced Updater) are affected by a remote code execution vulnerability via the CustomDetection parameter in the update check function. To exploit this vulnerability, a user must start an affected installation to trigger the update check.	8.1	More Details
CVE-2022-1987	Buffer Over-read in GitHub repository bfabiszewski/libmobi prior to 0.11.	8.1	More Details
CVE-2021-34083	Google-it is a Node.js package which allows its users to send search queries to Google and receive the results in a JSON format. When using the 'Open in browser' option in versions up to 1.6.2, google-it will unsafely concat the result's link retrieved from google to a shell command, potentially exposing the server to RCE.	8.1	More Details
CVE-2022-30232	A CWE-20: Improper Input Validation vulnerability exists that could cause potential remote code execution when an attacker is able to intercept and modify a request on the same network or has configuration access to an ION device on the network. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior)	8.0	More Details
CVE-2022-24701	An issue was discovered in WinAPRS 2.9.0. A buffer overflow in national.txt processing allows a local attacker to cause a denial of service or possibly achieve code execution. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	7.8	More Details
CVE-2022-29488	The affected product is vulnerable to an out-of-bounds read via uninitialized pointer, which may allow an attacker to execute arbitrary code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28690	The affected product is vulnerable to an out-of-bounds write via uninitialized pointer, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2022-1968	Use After Free in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-29692	Unicorn Engine v1.0.3 was discovered to contain a use-after-free vulnerability via the hook function.	7.8	More Details
CVE-2022-1943	A flaw out of bounds memory write in the Linux kernel UDF file system functionality was found in the way user triggers some file operation which triggers udf_write_fi(). A local user could use this flaw to crash the system or potentially	7.8	More Details
CVE-2022-27184	The affected product is vulnerable to an out-of-bounds write, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2022-30540	The affected product is vulnerable to a heap-based buffer overflow via uninitialized pointer, which may allow an attacker to execute arbitrary code	7.8	More Details
CVE-2022-29483	Incorrect Default Permissions vulnerability in ABB e-Design allows attacker to install malicious software executing with SYSTEM permissions violating confidentiality, integrity, and availability of the target machine.	7.8	More Details
CVE-2021-42197	An issue was discovered in swftools through 20201222 through a memory leak in the swftools when swfdump is used. It allows an attacker to cause code execution.	7.8	More Details
CVE-2022-30190	A remote code execution vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. The attacker can then install programs, view, change, or delete data, or create new accounts in the context allowed by the user's rights. Please see the MSRC Blog Entry for important information about steps you can take to protect your system from this vulnerability.	7.8	More Details
CVE-2021-42195	An issue was discovered in swftools through 20201222. A heap-buffer-overflow exists in the function handleEditText() located in swfdump.c. It allows an attacker to cause code Execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26635	In the code that verifies the file size in the ark library, it is possible to manipulate the offset read from the target file due to the wrong use of the data type. An attacker could use this vulnerability to cause a stack buffer overflow and as a result, perform an attack such as remote code execution.	7.8	More Details
CVE-2022-1786	A use-after-free flaw was found in the Linux kernel's io_uring subsystem in the way a user sets up a ring with IORING_SETUP_IOPOLL with more than one task completing submissions on this ring. This flaw allows a local user to crash or escalate their privileges on the system.	7.8	More Details
CVE-2021-42199	An issue was discovered in swftools through 20201222. A heap buffer overflow exists in the function swf_FontExtract_DefineTextCallback() located in swftext.c. It allows an attacker to cause code execution.	7.8	More Details
CVE-2021-42201	An issue was discovered in swftools through 20201222. A heap-buffer-overflow exists in the function swf_GetD64() located in rfxswf.c. It allows an attacker to cause code execution.	7.8	More Details
CVE-2021-42203	An issue was discovered in swftools through 20201222. A heap-use-after-free exists in the function swf_FontExtract_DefineTextCallback() located in swftext.c. It allows an attacker to cause code execution.	7.8	More Details
CVE-2021-42204	An issue was discovered in swftools through 20201222. A heap-buffer-overflow exists in the function swf_GetBits() located in rfxswf.c. It allows an attacker to cause code execution.	7.8	More Details
CVE-2022-32200	libdwarf 0.4.0 has a heap-based buffer over-read in _dwarf_check_string_valid in dwarf_util.c.	7.8	More Details
CVE-2022-31500	In KNIME Analytics Platform below 4.6.0, the Windows installer sets improper filesystem permissions.	7.8	More Details
CVE-2022-31782	ftbench.c in FreeType Demo Programs through 2.12.1 has a heap-based buffer overflow.	7.8	More Details
CVE-2022-32250	net/netfilter/nf_tables_api.c in the Linux kernel through 5.18.1 allows a local user (able to create user/net namespaces) to escalate privileges to root because an incorrect NFT_STATEFUL_EXPR check leads to a use-after-free.	7.8	More Details
CVE-2022-1215	A format string vulnerability was found in libinput	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1419	The root cause of this vulnerability is that the ioctl$DRM_IOCTL_MODE_DESTROY_DUMB can decrease refcount of *drm_vgem_gem_object *(created in *vgem_gem_dumb_create*) concurrently, and *vgem_gem_dumb_create *will access the freed drm_vgem_gem_object.	7.8	More Details
CVE-2022-1652	Linux Kernel could allow a local attacker to execute arbitrary code on the system, caused by a concurrency use-after-free flaw in the bad_flp_intr function. By executing a specially-crafted program, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.	7.8	More Details
CVE-2022-29594	eG Agent before 7.2 has weak file permissions that enable escalation of privileges to SYSTEM.	7.8	More Details
CVE-2022-1940	A Stored Cross-Site Scripting vulnerability in Jira integration in GitLab EE affecting all versions from 13.11 prior to 14.9.5, 14.10 prior to 14.10.4, and 15.0 prior to 15.0.1 allows an attacker to execute arbitrary JavaScript code in GitLab on a victim's behalf via specially crafted Jira Issues	7.7	More Details
CVE-2021-27914	A cross-site scripting (XSS) vulnerability in the installer component of Mautic before 4.3.0 allows admins to inject executable javascript	7.6	More Details
CVE-2022-31004	CVEProject/cve-services is an open source project used to operate the CVE services API. A conditional in 'data.js' has potential for production secrets to be written to disk. The affected method writes the generated randomKey to disk if the environment is not development. If this method were called in production, it is possible that it would write the plaintext key to disk. A patch is not available as of time of publication but is anticipated as a "hot fix" for version 1.1.1 and for the 2.x branch.	7.5	More Details
CVE-2022-31484	An unauthenticated attacker can send a specially crafted network packet to delete a user from the web interface. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.29. The impact of this vulnerability is that an unauthenticated attacker could restrict access to the web interface to legitimate users and potentially requiring them to use the default user dip switch procedure to gain access back.	7.5	More Details
CVE-2022-29631	Jodd HTTP v6.0.9 was discovered to contain multiple CLRF injection vulnerabilities via the components jodd.http.HttpRequest#set and `jodd.http.HttpRequest#send. These vulnerabilities allow attackers to execute Server-Side Request Forgery (SSRF) via a crafted TCP payload.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30587	Gradle Enterprise through 2022.2.2 has Incorrect Access Control that leads to information disclosure.	7.5	More Details
CVE-2022-21757	In WIFI Firmware, there is a possible system crash due to a missing count check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06468894; Issue ID: ALPS06468894.	7.5	More Details
CVE-2022-29693	Unicorn Engine v2.0.0-rc7 and below was discovered to contain a memory leak via the function uc_close at /my/unicorn/uc.c.	7.5	More Details
CVE-2022-29694	Unicorn Engine v2.0.0-rc7 and below was discovered to contain a NULL pointer dereference via qemu_ram_free.	7.5	More Details
CVE-2022-29695	Unicorn Engine v2.0.0-rc7 contains memory leaks caused by an incomplete unicorn engine initialization.	7.5	More Details
CVE-2022-29729	Verizon 4G LTE Network Extender GA4.38 - V0.4.038.2131 utilizes a weak default admin password generation algorithm which generates passwords that are accessible to unauthenticated attackers via the webUI login page.	7.5	More Details
CVE-2022-32275	Grafana 8.4.3 allows reading files via (for example) a /dashboard/snapshot/%7B%7Bconstructor.constructor'/.. /.. /.. /.. /.. /.. /.. /.. /etc/passwd URI. NOTE: the vendor's position is that there is no vulnerability; this request yields a benign error page, not /etc/passwd content	7.5	More Details
CVE-2022-22396	Credentials are printed in clear text in the IBM Spectrum Protect Plus 10.1.0.0 through 10.1.9.3 virgo log file in certain cases. Credentials could be the remote vSnap, offload targets, or VADP credentials depending on the operation performed. Credentials that are using API key or certificate are not printed. IBM X-Force ID: 222231.	7.5	More Details
CVE-2022-30496	SQL injection in Logon Page of IDCE MV's application, version 1.0, allows an attacker to inject SQL payloads in the user field, connecting to a database to access enterprise's private and sensitive information.	7.5	More Details
CVE-2021-42889	In TOTOLINK EX1200T V4.1.2cu.5215, an attacker can obtain sensitive information (wifikey, wifiname, etc.) without authorization.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23712	A Denial of Service flaw was discovered in Elasticsearch. Using this vulnerability, an unauthenticated attacker could forcibly shut down an Elasticsearch node with a specifically formatted network request.	7.5	More Details
CVE-2021-42886	TOTOLINK EX1200T V4.1.2cu.5215 contains an information disclosure vulnerability where an attacker can get the apmib configuration file without authorization, and usernames and passwords can be found in the decoded file.	7.5	More Details
CVE-2022-31482	An unauthenticated attacker can send a specially crafted unauthenticated HTTP request to the device that can overflow a buffer. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.29. The overflowed data leads to segmentation fault and ultimately a denial-of-service condition, causing the device to reboot. The impact of this vulnerability is that an unauthenticated attacker could leverage this flaw to cause the target device to become unresponsive. An attacker could automate this attack to achieve persistent DoS, effectively rendering the target controller useless.	7.5	More Details
CVE-2022-29169	BigBlueButton is an open source web conferencing system. Versions starting with 2.2 and prior to 2.3.19, 2.4.7, and 2.5.0-beta.2 are vulnerable to regular expression denial of service (ReDoS) attacks. By using specific a RegularExpression, an attacker can cause denial of service for the bbb-html5 service. The useragent library performs checking of device by parsing the input of User-Agent header and lets it go through lookupUserAgent() (alias of useragent.lookup()). This function handles input by regexing and attackers can abuse that by providing some ReDos payload using `SmartWatch`. The maintainers removed `htmlclient/useragent` from versions 2.3.19, 2.4.7, and 2.5.0-beta.2. As a workaround, disable NginX forwarding the requests to the handler according to the directions in the GitHub Security Advisory.	7.5	More Details
CVE-2022-24700	An issue was discovered in WinAPRS 2.9.0. A buffer overflow in DIGI address processing for VHF KISS packets allows a remote attacker to cause a denial of service (daemon crash) via a malicious AX.25 packet over the air. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1708	A vulnerability was found in CRI-O that causes memory or disk space exhaustion on the node for anyone with access to the Kube API. The ExecSync request runs commands in a container and logs the output of the command. This output is then read by CRI-O after command execution, and it is read in a manner where the entire file corresponding to the output of the command is read in. Thus, if the output of the command is large it is possible to exhaust the memory or the disk space of the node when CRI-O reads the output of the command. The highest threat from this vulnerability is system availability.	7.5	More Details
CVE-2022-27782	libcurl would reuse a previously created connection even when a TLS or SSHrelated option had been changed that should have prohibited reuse.libcurl keeps previously used connections in a connection pool for subsequenttransfers to reuse if one of them matches the setup. However, several TLS andSSH settings were left out from the configuration match checks, making themmatch too easily.	7.5	More Details
CVE-2021-33254	An issue was discovered in src/http/httpLib.c in EmbedThis Appweb Community Edition 8.2.1, allows attackers to cause a denial of service via the stream paramter to the parseUri function.	7.5	More Details
CVE-2022-1661	The affected products are vulnerable to directory traversal, which may allow an attacker to obtain arbitrary operating system files.	7.5	More Details
CVE-2021-26633	SQL injection and Local File Inclusion (LFI) vulnerabilities in MaxBoard can cause information leakage and privilege escalation. This vulnerabilities can be exploited by manipulating a variable with a desired value and inserting and arbitrary file.	7.5	More Details
CVE-2022-22557	PowerStore contains Plain-Text Password Storage Vulnerability in PowerStore X & T environments running versions 2.0.0.x and 2.0.1.x A locally authenticated attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	7.5	More Details
CVE-2022-30746	Missing caller check in Smart Things prior to version 1.7.85.12 allows attacker to access senstive information remotely using javascript interface API.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1949	An access control bypass vulnerability found in 389-ds-base. That mishandling of the filter that would yield incorrect results, but as that has progressed, can be determined that it actually is an access control bypass. This may allow any remote unauthenticated user to issue a filter that allows searching for database items they do not have access to, including but not limited to potentially userPassword hashes and other sensitive data.	7.5	More Details
CVE-2021-42893	In TOTOLINK EX1200T V4.1.2cu.5215, an attacker can obtain sensitive information (wifikey, etc.) without authorization through getSysStatusCfg.	7.5	More Details
CVE-2021-42877	TOTOLINK EX1200T V4.1.2cu.5215 contains a denial of service vulnerability in function RebootSystem of the file lib/cste_modules/system which can reboot the system.	7.5	More Details
CVE-2022-24241	ACEweb Online Portal 3.5.065 was discovered to contain an External Controlled File Path and Name vulnerability via the txtFilePath parameter in attachments.awp.	7.5	More Details
CVE-2021-42891	In TOTOLINK EX1200T V4.1.2cu.5215, an attacker can obtain sensitive information (wifikey, etc.) without authorization.	7.5	More Details
CVE-2022-24581	ACEweb Online Portal 3.5.065 allows unauthenticated SMB hash capture via UNC. By specifying the UNC file path of an external SMB share when uploading a file, an attacker can induce the victim server to disclose the username and password hash of the user executing the ACEweb Online software.	7.5	More Details
CVE-2021-33615	RSA Archer 6.8.00500.1003 P5 allows Unrestricted Upload of a File with a Dangerous Type.	7.5	More Details
CVE-2022-31480	An unauthenticated attacker could arbitrarily upload firmware files to the target device, ultimately causing a Denial-of-Service (DoS). This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.302 for the LP series and 1.296 for the EP series. The attacker needs to have a properly signed and encrypted binary, loading the firmware to the device ultimately triggers a reboot.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31018	Play Framework is a web framework for Java and Scala. A denial of service vulnerability has been discovered in verions 2.8.3 through 2.8.15 of Play's forms library, in both the Scala and Java APIs. This can occur when using either the `Form#bindFromRequest` method on a JSON request body or the `Form#bind` method directly on a JSON value. If the JSON data being bound to the form contains a deeply-nested JSON object or array, the form binding implementation may consume all available heap space and cause an `OutOfMemoryError`. If executing on the default dispatcher and `akka.jvm-exit-on-fatal-error` is enabled—as it is by default—then this can crash the application process. `Form.bindFromRequest` is vulnerable when using any body parser that produces a type of `AnyContent` or `JsValue` in Scala, or one that can produce a `JsonNode` in Java. This includes Play's default body parser. This vulnerability been patched in version 2.8.16. There is now a global limit on the depth of a JSON object that can be parsed, which can be configured by the user if necessary. As a workaround, applications that do not need to parse a request body of type `application/json` can switch from the default body parser to another body parser that supports only the specific type of body they expect.	7.5	More Details
CVE-2022-31028	MinIO is a multi-cloud object storage solution. Starting with version RELEASE.2019-09-25T18-25-51Z and ending with version RELEASE.2022-06-02T02-11-04Z, MinIO is vulnerable to an unending go-routine buildup while keeping connections established due to HTTP clients not closing the connections. Public-facing MinIO deployments are most affected. Users should upgrade to RELEASE.2022-06-02T02-11-04Z to receive a patch. One possible workaround is to use a reverse proxy to limit the number of connections being attempted in front of MinIO, and actively rejecting connections from such malicious clients.	7.5	More Details
CVE-2022-27781	libcurl provides the `CURLOPT_CERTINFO` option to allow applications torequest details to be returned about a server's certificate chain.Due to an erroneous function, a malicious server could make libcurl built withNSS get stuck in a never-ending busy-loop when trying to retrieve thatinformation.	7.5	More Details
CVE-2022-26975	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing log files without authentication.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27780	The curl URL parser wrongly accepts percent-encoded URL separators like '/'when decoding the host name part of a URL, making it a *different* URL usingthe wrong host name when it is later retrieved.For example, a URL like `http://example.com%2F127.0.0.1/`, would be allowed bythe parser and get transposed into `http://example.com/127.0.0.1/`. This flawcan be used to circumvent filters, checks and more.	7.5	More Details
CVE-2022-29564	Jamf Private Access before 2022-05-16 has Incorrect Access Control, in which an unauthorized user can reach a system in the internal infrastructure, aka WND-44801.	7.5	More Details
CVE-2020-26185	Dell BSAFE Micro Edition Suite, versions prior to 4.5.1, contain a Buffer Over-Read Vulnerability.	7.5	More Details
CVE-2021-37589	Virtua Cobranca before 12R allows SQL Injection on the login page.	7.5	More Details
CVE-2020-26184	Dell BSAFE Micro Edition Suite, versions prior to 4.5.1, contain an Improper Certificate Validation vulnerability.	7.5	More Details
CVE-2022-27775	An information disclosure vulnerability exists in curl 7.65.0 to 7.82.0 are vulnerable that by using an IPv6 address that was in the connection pool but with a different zone id it could reuse a connection instead.	7.5	More Details
CVE-2022-31459	Owl Labs Meeting Owl 5.2.0.15 allows attackers to retrieve the passcode hash via a certain c 10 value over Bluetooth.	7.4	More Details
CVE-2022-31460	Owl Labs Meeting Owl 5.2.0.15 allows attackers to activate Tethering Mode with hard-coded hoothoot credentials via a certain c 150 value.	7.4	More Details
CVE-2022-31461	Owl Labs Meeting Owl 5.2.0.15 allows attackers to deactivate the passcode protection mechanism via a certain c 11 message.	7.4	More Details
CVE-2020-36542	A vulnerability classified as critical has been found in Demokratian. This affects an unknown part of the file install/install3.php. The manipulation leads to privilege escalation. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36541	A vulnerability was found in Demokratian. It has been rated as critical. Affected by this issue is some unknown functionality of the file basicos_php/genera_select.php. The manipulation of the argument id_provincia with the input -1%20union%20all%20select%201,2,3,4,database() leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue.	7.3	More Details
CVE-2022-32003	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/courts/view_court.php?id=.	7.2	More Details
CVE-2022-31983	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/admin/?page=requests/manage_request&id=.	7.2	More Details
CVE-2022-32006	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/services/view_service.php?id=.	7.2	More Details
CVE-2022-32005	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/admin/services/manage_service.php?id=.	7.2	More Details
CVE-2022-32004	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/admin/products/manage_product.php?id=.	7.2	More Details
CVE-2022-31981	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/admin/?page=teams/view_team&id=.	7.2	More Details
CVE-2022-31982	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/admin/?page=requests/view_request&id=.	7.2	More Details
CVE-2022-32000	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page=service_transactions/manage_service_transaction&id=.	7.2	More Details
CVE-2022-31980	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/admin/?page=teams/manage_team&id=.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31998	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page=service_transactions/view_details&id=.	7.2	More Details
CVE-2022-31996	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/admin/?page=sales/manage_sale&id=.	7.2	More Details
CVE-2022-31984	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/admin/requests/take_action.php?id=.	7.2	More Details
CVE-2022-31985	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page=reports/daily_sales_report&date=.	7.2	More Details
CVE-2022-32001	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/admin/products/view_product.php?id=.	7.2	More Details
CVE-2022-32027	Car Rental Management System v1.0 is vulnerable to SQL Injection via /car-rental-management-system/admin/index.php?page=manage_car&id=.	7.2	More Details
CVE-2022-31986	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page=reports/daily_court_rental_report&date=.	7.2	More Details
CVE-2022-32016	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/index.php?q=result&searchfor=bycompany.	7.2	More Details
CVE-2022-32026	Car Rental Management System v1.0 is vulnerable to SQL Injection via /car-rental-management-system/admin/manage_booking.php?id=.	7.2	More Details
CVE-2022-32028	Car Rental Management System v1.0 is vulnerable to SQL Injection via /car-rental-management-system/admin/manage_user.php?id=.	7.2	More Details
CVE-2022-32025	Car Rental Management System v1.0 is vulnerable to SQL Injection via /car-rental-management-system/admin/view_car.php?id=.	7.2	More Details
CVE-2022-31974	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/admin/?page=reports&date=.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32024	Car Rental Management System v1.0 is vulnerable to SQL Injection via car-rental-management-system/booking.php?car_id=.	7.2	More Details
CVE-2022-32022	Car Rental Management System v1.0 is vulnerable to SQL Injection via /ip/car-rental-management-system/admin/ajax.php?action=login.	7.2	More Details
CVE-2022-32021	Car Rental Management System v1.0 is vulnerable to SQL Injection via /car-rental-management-system/admin/manage_movement.php?id=.	7.2	More Details
CVE-2022-30860	FUDforum 3.1.2 is vulnerable to Remote Code Execution through Upload File feature of File Administration System in Admin Control Panel.	7.2	More Details
CVE-2022-32018	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/index.php?q=hiring&search=.	7.2	More Details
CVE-2022-32015	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/index.php?q=category&search=.	7.2	More Details
CVE-2022-31988	Badminton Center Management System v1.0 is vulnerable to SQL Injection via bcms/admin/?page=reports/daily_services_report&date=.	7.2	More Details
CVE-2022-32014	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/index.php?q=result&searchfor=byfunction.	7.2	More Details
CVE-2022-32013	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via eris/admin/category/index.php?view=edit&id=.	7.2	More Details
CVE-2022-32012	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/admin/employee/index.php?view=edit&id=.	7.2	More Details
CVE-2022-32011	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/admin/applicants/index.php?view=view&id=.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32010	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/admin/user/index.php?view=edit&id=.	7.2	More Details
CVE-2022-32008	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via eris/admin/vacancy/index.php?view=edit&id=.	7.2	More Details
CVE-2022-32007	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/admin/company/index.php?view=edit&id=.	7.2	More Details
CVE-2022-31994	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page=sales/view_details&id.	7.2	More Details
CVE-2022-31992	Badminton Center Management System v1.0 is vulnerable to SQL Injection via /bcms/admin/?page=court_rentals/view_court_rental&id=.	7.2	More Details
CVE-2022-31975	Online Fire Reporting System v1.0 is vulnerable to SQL Injection via /ofrs/admin/?page=user/manage_user&id=.	7.2	More Details
CVE-2022-32017	Complete Online Job Search System v1.0 is vulnerable to SQL Injection via /eris/index.php?q=result&searchfor=bytitle.	7.2	More Details
CVE-2022-30798	Online Ordering System v1.0 by oretnom23 is vulnerable to SQL Injection via admin/viewreport.php.	7.2	More Details
CVE-2022-30830	Wedding Management System v1.0 is vulnerable to SQL Injection via \admin\feature_edit.php.	7.2	More Details
CVE-2022-30586	Gradle Enterprise through 2022.2.2 has Incorrect Access Control that leads to code execution.	7.2	More Details
CVE-2022-30794	Online Ordering System v1.0 by oretnom23 is vulnerable to SQL Injection via admin/editproductetails.php.	7.2	More Details
CVE-2022-30795	Online Ordering System v1.0 by oretnom23 is vulnerable to SQL Injection via admin/editproductimage.php.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44080	A Command Injection vulnerability in httpd web server (setup.cgi) in SerComm h500s, FW: lowi-h500s-v3.4.22 allows logged in administrators to arbitrary OS commands as root in the device via the connection_type parameter of the statussupport_diagnostic_tracing.json endpoint.	7.2	More Details
CVE-2022-30799	Online Ordering System v1.0 by oretnom23 has SQL injection via store/orderpage.php.	7.2	More Details
CVE-2022-30818	Wedding Management System v1.0 is vulnerable to SQL injection via /Wedding-Management/admin/blog_events_edit.php?id=31.	7.2	More Details
CVE-2022-30823	Wedding Management System v1.0 is vulnerable to SQL Injection via \admin\blog_events_edit.php.	7.2	More Details
CVE-2022-30825	Wedding Management System v1.0 is vulnerable to SQL Injection via \admin\client_edit.php.	7.2	More Details
CVE-2022-30826	Wedding Management System v1.0 is vulnerable to SQL Injection via admin\client_assign.php.	7.2	More Details
CVE-2022-30827	Wedding Management System v1.0 is vulnerable to SQL Injection via \admin\package_edit.php.	7.2	More Details
CVE-2022-30829	Wedding Management System v1.0 is vulnerable to SQL Injection via \admin\users_edit.php.	7.2	More Details
CVE-2022-30828	Wedding Management System v1.0 is vulnerable to SQL Injection via \admin\photos_edit.php.	7.2	More Details
CVE-2022-30831	Wedding Management System v1.0 is vulnerable to SQL Injection via Wedding-Management/wedding_details.php.	7.2	More Details
CVE-2022-30832	Wedding Management System v1.0 is vulnerable to SQL Injection via /Wedding-Management/admin/client_assign.php?booking=31&user_id=.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30833	Wedding Management System v1.0 is vulnerable to SQL Injection via /Wedding-Management/admin/client_edit.php?booking=31&user_id=.	7.2	More Details
CVE-2022-30834	Wedding Management System v1.0 is vulnerable to SQL Injection via /Wedding-Management/admin/client_manage_account_details.php?booking_id=31&user_id=	7.2	More Details
CVE-2022-30835	Wedding Management System v1.0 is vulnerable to SQL Injection. via /Wedding-Management/admin/budget.php?booking_id=.	7.2	More Details
CVE-2022-30836	Wedding Management System v1.0 is vulnerable to SQL Injection. via Wedding-Management/admin/select.php.	7.2	More Details
CVE-2022-31339	Simple Inventory System v1.0 is vulnerable to SQL Injection via /inventory/login.php.	7.2	More Details
CVE-2022-31971	ChatBot App with Suggestion v1.0 is vulnerable to SQL Injection via /simple_chat_bot/admin/?page=responses/view_response&id=.	7.2	More Details
CVE-2022-31970	ChatBot App with Suggestion v1.0 is vulnerable to SQL Injection via /simple_chat_bot/admin/?page=responses/manage_response&id=.	7.2	More Details
CVE-2021-43271	Riverbed AppResponse 11.8.0, 11.8.5, 11.8.5a, 11.9.0, 11.9.0a, 11.10.0, 11.11.0, 11.11.0a, 11.11.1, 11.11.1a, 11.11.5, and 11.11.5a (when configured to use local, RADIUS, or TACACS authentication) logs usernames and passwords if either is entered incorrectly. If a user enters an incorrect username and/or password when logging into the WebUI, these attempted credentials are included in an error message that is logged in the WebUI log file. A log entry does not appear if the username and password provided correctly match a valid set of credentials. This also does not happen if AppResponse is configured to use SAML authentication. The WebUI log file is included in subsequent diagnostic system dumps that are generated. (Only users with Full Control access to the System Configuration permission can generate system dumps. By default, only System Administrators have Full Control access to the System Configuration permission.)	6.8	More Details
CVE-2022-1789	With shadow paging enabled, the INVPCID instruction results in a call to kvm_mmu_invpcid_gva. If INVPCID is executed with CR0.PG=0, the invlpg callback is not set and the result is a NULL pointer dereference.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1797	A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition in Rockwell Automation Logix Controllers, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online.	6.8	More Details
CVE-2022-21758	In ccu, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06439600; Issue ID: ALPS06439600.	6.7	More Details
CVE-2022-21759	In power service, 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: ALPS06419106; Issue ID: ALPS06419077.	6.7	More Details
CVE-2021-35531	Improper Input Validation vulnerability in a particular configuration setting field of Hitachi Energy TXpert Hub CoreTec 4 product, allows an attacker with access to an authorized user with ADMIN or ENGINEER role rights to inject an OS command that is executed by the system. This issue affects: Hitachi Energy TXpert Hub CoreTec 4 version 2.0.0; 2.0.1; 2.1.0; 2.1.1; 2.1.2; 2.1.3; 2.2.0; 2.2.1.	6.7	More Details
CVE-2021-35532	A vulnerability exists in the file upload validation part of Hitachi Energy TXpert Hub CoreTec 4 product. The vulnerability allows an attacker or malicious agent who manages to gain access to the system and obtain an account with sufficient privilege to upload a malicious firmware to the product. This issue affects: Hitachi Energy TXpert Hub CoreTec 4 version 2.0.0; 2.0.1; 2.1.0; 2.1.1; 2.1.2; 2.1.3; 2.2.0; 2.2.1.	6.7	More Details
CVE-2022-21753	In WLAN driver, 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: ALPS06493873; Issue ID: ALPS06493899.	6.7	More Details
CVE-2022-21754	In WLAN driver, 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: ALPS06535953; Issue ID: ALPS06535953.	6.7	More Details
CVE-2022-21752	In WLAN driver, 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: ALPS06493873; Issue ID: ALPS06493873.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21751	In WLAN driver, 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: ALPS06511132; Issue ID: ALPS06511132.	6.7	More Details
CVE-2022-21750	In WLAN driver, 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: ALPS06521283; Issue ID: ALPS06521283.	6.7	More Details
CVE-2022-30233	A CWE-20: Improper Input Validation vulnerability exists that could allow the product to be maliciously manipulated when the user is tricked into performing certain actions on a webpage. Affected Products: Wiser Smart, EER21000 & EER21001 (V4.5 and prior)	6.5	More Details
CVE-2021-40186	The AppCheck research team identified a Server-Side Request Forgery (SSRF) vulnerability within the DNN CMS platform, formerly known as DotNetNuke. SSRF vulnerabilities allow the attacker to exploit the target system to make network requests on their behalf, allowing a range of possible attacks. In the most common scenario, the attacker exploits SSRF vulnerabilities to attack systems behind the firewall and access sensitive information from Cloud Provider metadata services.	6.5	More Details
CVE-2022-1935	Incorrect authorization in GitLab EE affecting all versions from 12.0 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting from 15.0 before 15.0.1 allowed an attacker already in possession of a valid Project Trigger Token to misuse it from any location even when IP address restrictions were configured	6.5	More Details
CVE-2022-29767	adbyby v2.7 allows external users to make connections via port 8118. This can cause a program logic error and lead to a Denial of Service (DoS) via high CPU usage due to a large number of connections.	6.5	More Details
CVE-2022-29773	An access control issue in aleksis/core/util/auth_helpers.py: ClientProtectedResourceMixin of AlekSIS-Core v2.8.1 and below allows attackers to access arbitrary scopes if no allowed scopes are specifically set.	6.5	More Details
CVE-2022-29232	BigBlueButton is an open source web conferencing system. Starting with version 2.2 and prior to versions 2.3.9 and 2.4-beta-1, an attacker can circumvent access controls to obtain the content of public chat messages from different meetings on the server. The attacker must be a participant in a meeting on the server. BigBlueButton versions 2.3.9 and 2.4-beta-1 contain a patch for this issue. There are currently no known workarounds.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29620	FileZilla v3.59.0 allows attackers to obtain cleartext passwords of connected SSH or FTP servers via a memory dump.- NOTE: the vendor does not consider this a vulnerability	6.5	More Details
CVE-2022-30466	joyebike Joy ebike Wolf Manufacturing year 2022 is vulnerable to Authentication Bypass by Capture-replay.	6.5	More Details
CVE-2022-31024	richdocuments is the repository for NextCloud Collabra, the app for Nextcloud Office collaboration. Prior to versions 6.0.0, 5.0.4, and 4.2.6, a user could be tricked into working against a remote Office by sending them a federated share. richdocuments versions 6.0.0, 5.0.4 and 4.2.6 contain a fix for this issue. There are currently no known workarounds available.	6.5	More Details
CVE-2022-29597	Solutions Atlantic Regulatory Reporting System (RRS) v500 is vulnerable to Local File Inclusion (LFI). Any authenticated user has the ability to reference internal system files within requests made to the RRSWeb/maint/ShowDocument/ShowDocument.aspx page. The server will successfully respond with the file contents of the internal system file requested. This ability could allow for adversaries to extract sensitive data and/or files from the underlying file system, gain knowledge about the internal workings of the system, or access source code of the application.	6.5	More Details
CVE-2022-26944	Percona XtraBackup 2.4.20 unintentionally writes the command line to any resulting backup file output. This may include sensitive arguments passed at run time. In addition, when --history is passed at run time, this command line is also written to the PERCONA_SCHEMA.xtrabackup_history table. NOTE: this issue exists because of an incomplete fix for CVE-2020-10997.	6.5	More Details
CVE-2022-31973	Online Fire Reporting System v1.0 is vulnerable to Delete any file via /ofrs/classes/Master.php?f=delete_img.	6.5	More Details
CVE-2022-1936	Incorrect authorization in GitLab EE affecting all versions from 12.0 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting from 15.0 before 15.0.1 allowed an attacker already in possession of a valid Project Deploy Token to misuse it from any location even when IP address restrictions were configured	6.5	More Details
CVE-2022-27776	A insufficiently protected credentials vulnerability in fixed in curl 7.83.0 might leak authentication or cookie header data on HTTP redirects to the same host but another port number.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30804	elitecms v1.01 is vulnerable to Delete any file via /admin/delete_image.php?file=.	6.5	More Details
CVE-2022-29617	Due to improper error handling an authenticated user can crash CLA assistant instance. This could impact the availability of the application.	6.5	More Details
CVE-2022-31342	Online Car Wash Booking System v1.0 is vulnerable to Delete any file via /ocwbs/classes/Master.php?f=delete_img.	6.5	More Details
CVE-2022-29788	libmobi before v0.10 contains a NULL pointer dereference via the component mobi_buffer_getpointer. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted mobi file.	6.5	More Details
CVE-2022-28478	SeedDMS 6.0.17 and 5.1.24 are vulnerable to Directory Traversal. The "Remove file" functionality inside the "Log files management" menu does not sanitize user input allowing attackers with admin privileges to delete arbitrary files on the remote system.	6.5	More Details
CVE-2022-1285	Server-Side Request Forgery (SSRF) in GitHub repository gogs/gogs prior to 0.12.8.	6.5	More Details
CVE-2022-24967	Black Rainbow NIMBUS before 3.7.0 allows stored Cross-site Scripting (XSS).	6.5	More Details
CVE-2022-31796	libjpeg 1.63 has a heap-based buffer over-read in HierarchicalBitmapRequester::FetchRegion in hierarchicalbitmaprequester.cpp because the MCU size can be different between allocation and use.	6.5	More Details
CVE-2022-31966	ChatBot App with Suggestion v1.0 is vulnerable to Delete any file via /simple_chat_bot/classes/Master.php?f=delete_img.	6.5	More Details
CVE-2022-26868	Dell EMC PowerStore versions 2.0.0.x, 2.0.1.x, and 2.1.0.x are vulnerable to a command injection flaw. An authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system takeover by an attacker.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29085	Dell Unity, Dell UnityVSA, and Dell Unity XT versions prior to 5.2.0.0.5.173 contain a plain-text password storage vulnerability when certain off-array tools are run on the system. The credentials of a user with high privileges are stored in plain text. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user.	6.4	More Details
CVE-2020-36537	A vulnerability was found in Everywhere CMS. It has been classified as critical. Affected is an unknown function. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely.	6.3	More Details
CVE-2020-36539	A vulnerability was found in Lógico y Creativo 1.0 and classified as critical. This issue affects some unknown processing. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely.	6.3	More Details
CVE-2020-36530	A vulnerability classified as critical was found in SevOne Network Management System up to 5.7.2.22. This vulnerability affects the Alert Summary. The manipulation leads to sql injection. The attack can be initiated remotely.	6.3	More Details
CVE-2020-36540	A vulnerability, which was classified as critical, was found in Neetai Tech. Affected is an unknown function of the file /product.php. The manipulation leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2020-36531	A vulnerability, which was classified as critical, has been found in SevOne Network Management System up to 5.7.2.22. This issue affects the Device Manager Page. An injection leads to privilege escalation. The attack may be initiated remotely.	6.3	More Details
CVE-2020-36538	A vulnerability was found in Eatan CMS. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. The attack can be launched remotely.	6.3	More Details
CVE-2020-36535	A vulnerability classified as critical has been found in MINMAX. This affects an unknown part of the file /newsDia.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely.	6.3	More Details
CVE-2020-36536	A vulnerability was found in Brandbugle. It has been rated as critical. Affected by this issue is some unknown functionality of the file /main.php. The manipulation leads to sql injection. The attack may be launched remotely.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1462	An out-of-bounds read flaw was found in the Linux kernel's TeleTYpe subsystem. The issue occurs in how a user triggers a race condition using ioctls TIOCSPTLCK and TIOCGPTPEER and TIOCSTI and TCXONC with leakage of memory in the flush_to_ldisc function. This flaw allows a local user to crash the system or read unauthorized random data from memory.	6.3	More Details
CVE-2022-31022	Bleve is a text indexing library for go. Bleve includes HTTP utilities under bleve/http package, that are used by its sample application. These HTTP methods pave way for exploitation of a node's filesystem where the bleve index resides, if the user has used bleve's own HTTP (bleve/http) handlers for exposing the access to the indexes. For instance, the CreateIndexHandler (`http/index_create.go`) and DeleteIndexHandler (`http/index_delete.go`) enable an attacker to create a bleve index (directory structure) anywhere where the user running the server has the write permissions and to delete recursively any directory owned by the same user account. Users who have used the bleve/http package for exposing access to bleve index without the explicit handling for the Role Based Access Controls(RBAC) of the index assets would be impacted by this issue. There is no patch for this issue because the http package is purely intended to be used for demonstration purposes. Bleve was never designed handle the RBACs, nor it was ever advertised to be used in that way. The collaborators of this project have decided to stay away from adding any authentication or authorization to bleve project at the moment. The bleve/http package is mainly for demonstration purposes and it lacks exhaustive validation of the user inputs as well as any authentication and authorization measures. It is recommended to not use bleve/http in production use cases.	6.2	More Details
CVE-2022-30722	Implicit Intent hijacking vulnerability in Samsung Account prior to SMR Jun-2022 Release 1 allows attackers to bypass user confirmation of Samsung Account.	6.2	More Details
CVE-2022-30726	Unprotected component vulnerability in DeviceSearchTrampoline in SecSettingsIntelligence prior to SMR Jun-2022 Release 1 allows local attackers to launch activities of SecSettingsIntelligence.	6.2	More Details
CVE-2022-30727	Improper handling of insufficient permissions vulnerability in addAppPackageNameToAllowList in PersonaManagerService prior to SMR Jun-2022 Release 1 allows local attackers to set some setting value in work space.	6.2	More Details
CVE-2022-30744	DLL hijacking vulnerability in KiesWrapper in Samsung Kies prior to version 2.6.4.22043_1 allows attacker to execute arbitrary code.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31492	Cross Site scripting (XSS) vulnerability inLibreHealth EHR Base 2.0.0 via interface/usergroup/usergroup_admin_add.php Username.	6.1	More Details
CVE-2022-31493	LibreHealth EHR Base 2.0.0 allows gacl/admin/acl_admin.php acl_id XSS.	6.1	More Details
CVE-2022-31498	LibreHealth EHR Base 2.0.0 allows interface/orders/patient_match_dialog.php key XSS.	6.1	More Details
CVE-2022-31494	LibreHealth EHR Base 2.0.0 allows gacl/admin/acl_admin.php action XSS.	6.1	More Details
CVE-2022-31495	LibreHealth EHR Base 2.0.0 allows gacl/admin/acl_admin.php return_page XSS.	6.1	More Details
CVE-2021-42245	FlatCore-CMS 2.0.9 has a cross-site scripting (XSS) vulnerability in pages.edit.php through meta tags and content sections.	6.1	More Details
CVE-2022-29296	A reflected cross-site scripting (XSS) vulnerability in the login portal of Avantune Genialcloud ProJ - 10 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2022-31470	An XSS vulnerability in the index_mobile_changepass.hsp reset-password section of Axigen Mobile WebMail before 10.2.3.12 and 10.3.x before 10.3.3.47 allows attackers to run arbitrary Javascript code that, using an active end-user session (for a logged-in user), can access and retrieve mailbox content.	6.1	More Details
CVE-2022-1988	Cross-site Scripting (XSS) - Generic in GitHub repository neorazorx/facturascripts prior to 2022.09.	6.1	More Details
CVE-2022-30514	School Dormitory Management System v1.0 is vulnerable to reflected cross-site scripting (XSS) via admin/inc/navigation.php:126.	6.1	More Details
CVE-2022-26977	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a license file upload mechanism. Lack of input sanitization of the upload mechanism is leads to stored XSS.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26978	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a URL /checklogin.jsp endpoint. The os_username parameters is not correctly sanitized, leading to reflected XSS.	6.1	More Details
CVE-2022-26972	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a URL /cgi-bin endpoint. The URL parameters are not correctly sanitized, leading to reflected XSS.	6.1	More Details
CVE-2022-28702	Incorrect Default Permissions vulnerability in ABB e-Design allows attacker to install malicious software executing with SYSTEM permissions violating confidentiality, integrity, and availability of the target machine.	6.1	More Details
CVE-2022-29540	resi-calltrace in RESI Gemini-Net 4.2 is affected by Multiple XSS issues. Unauthenticated remote attackers can inject arbitrary web script or HTML into an HTTP GET parameter that reflects user input without sanitization. This exists on numerous application endpoints,	6.1	More Details
CVE-2022-29598	Solutions Atlantic Regulatory Reporting System (RRS) v500 is vulnerable to an reflected Cross-Site Scripting (XSS) vulnerability via RRSWeb/maint/ShowDocument/ShowDocument.aspx .	6.1	More Details
CVE-2022-29653	OFCMS v1.1.4 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /admin/comn/service/update.json.	6.1	More Details
CVE-2022-29711	LibreNMS v22.3.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /Table/GraylogController.php.	6.1	More Details
CVE-2022-29732	Delta Controls enteliTOUCH 3.40.3935, 3.40.3706, and 3.33.4005 was discovered to contain a cross-site scripting (XSS) vulnerability via the Username parameter. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2022-24238	ACEweb Online Portal 3.5.065 was discovered to contain a cross-site scripting (XSS) vulnerability via the txtNmName1 parameter in person.awp.	6.1	More Details
CVE-2022-23237	E-Series SANtricity OS Controller Software 11.x versions through 11.70.2 are vulnerable to host header injection attacks that could allow an attacker to redirect users to malicious websites.	6.1	More Details
CVE-2022-30349	siteserver SSCMS 6.15.51 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30513	School Dormitory Management System v1.0 is vulnerable to reflected cross-site scripting (XSS) via admin/inc/navigation.php:125	6.1	More Details
CVE-2022-26974	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a file upload mechanism. Lack of input sanitization in the upload mechanism leads to reflected XSS.	6.1	More Details
CVE-2022-29718	Caddy v2.4 was discovered to contain an open redirect vulnerability. A remote unauthenticated attacker may exploit this vulnerability to redirect users to arbitrary web URLs by tricking the victim users to click on crafted links.	6.1	More Details
CVE-2021-35530	A vulnerability in the application authentication and authorization mechanism in Hitachi Energy's TXpert Hub CoreTec 4, that depends on a token validation of the session identifier, allows an unauthorized modified message to be executed in the server enabling an unauthorized actor to change an existing user password, and further gain authorized access into the system via login mechanism. This issue affects: Hitachi Energy TXpert Hub CoreTec 4 version 2.0.0 2.1.0; 2.1.0; 2.1.1; 2.1.2; 2.1.3; 2.2.0; 2.2.1.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31023	Play Framework is a web framework for Java and Scala. Verions prior to 2.8.16 are vulnerable to generation of error messages containing sensitive information. Play Framework, when run in dev mode, shows verbose errors for easy debugging, including an exception stack trace. Play does this by configuring its `DefaultHttpErrorHandler` to do so based on the application mode. In its Scala API Play also provides a static object `DefaultHttpErrorHandler` that is configured to always show verbose errors. This is used as a default value in some Play APIs, so it is possible to inadvertently use this version in production. It is also possible to improperly configure the `DefaultHttpErrorHandler` object instance as the injected error handler. Both of these situations could result in verbose errors displaying to users in a production application, which could expose sensitive information from the application. In particular, the constructor for `CORSFilter` and `apply` method for `CORSActionBuilder` use the static object `DefaultHttpErrorHandler` as a default value. This is patched in Play Framework 2.8.16. The `DefaultHttpErrorHandler` object has been changed to use the prod-mode behavior, and `DevHttpErrorHandler` has been introduced for the dev-mode behavior. A workaround is available. When constructing a `CORSFilter` or `CORSActionBuilder`, ensure that a properly-configured error handler is passed. Generally this should be done by using the `HttpErrorHandler` instance provided through dependency injection or through Play's `BuiltInComponents`. Ensure that the application is not using the `DefaultHttpErrorHandler` static object in any code that may be run in production.	5.9	More Details
CVE-2021-43308	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the markdown-link-extractor npm package, when an attacker is able to supply arbitrary input to the module's exported function	5.9	More Details
CVE-2022-1929	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the devcert npm package, when an attacker is able to supply arbitrary input to the certificateFor method	5.9	More Details
CVE-2022-29733	Delta Controls enteliTOUCH 3.40.3935, 3.40.3706, and 3.33.4005 was discovered to transmit and store sensitive information in cleartext. This vulnerability allows attackers to intercept HTTP Cookie authentication credentials via a man-in-the-middle attack.	5.9	More Details
CVE-2021-43306	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the jquery-validation npm package, when an attacker is able to supply arbitrary input to the url2 method	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26491	An issue was discovered in Pidgin before 2.14.9. A remote attacker who can spoof DNS responses can redirect a client connection to a malicious server. The client will perform TLS certificate verification of the malicious domain name instead of the original XMPP service domain, allowing the attacker to take over control over the XMPP connection and to obtain user credentials and all communication content. This is similar to CVE-2022-24968.	5.9	More Details
CVE-2021-43307	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the semver-regex npm package, when an attacker is able to supply arbitrary input to the test() method	5.9	More Details
CVE-2022-26867	PowerStore SW v2.1.1.0 supports the option to export data to either a CSV or an XLSX file. The data is taken as is, without any validation or sanitization. It allows a malicious, authenticated user to inject payloads that might get interpreted as formulas by the corresponding spreadsheet application that is being used to open the CSV/XLSX file.	5.9	More Details
CVE-2022-30735	Improper privilege management vulnerability in Samsung Account prior to 13.2.00.6 allows attackers to get the access_token without permission.	5.9	More Details
CVE-2022-27774	An insufficiently protected credentials vulnerability exists in curl 4.9 to and include curl 7.82.0 are affected that could allow an attacker to extract credentials when follows HTTP(S) redirects is used with authentication could leak credentials to other services that exist on different protocols or port numbers.	5.7	More Details
CVE-2022-30277	BD Synapsys™, versions 4.20, 4.20 SR1, and 4.30, contain an insufficient session expiration vulnerability. If exploited, threat actors may be able to access, modify or delete sensitive information, including electronic protected health information (ePHI), protected health information (PHI) and personally identifiable information (PII).	5.7	More Details
CVE-2020-36528	A vulnerability, which was classified as critical, was found in Platinum Mobile 1.0.4.850. Affected is /MobileHandler.ashx which leads to broken access control. The attack requires authentication. Upgrading to version 1.0.4.851 is able to address this issue. It is recommended to upgrade the affected component.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26866	Dell PowerStore Versions before v2.1.1.0. contains a Stored Cross-Site Scripting vulnerability. A high privileged network attacker could potentially exploit this vulnerability, leading to the storage of malicious HTML or JavaScript codes in a trusted application data store. When a victim user accesses the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery.	5.5	More Details
CVE-2022-28224	Clusters using Calico (version 3.22.1 and below), Calico Enterprise (version 3.12.0 and below), may be vulnerable to route hijacking with the floating IP feature. Due to insufficient validation, a privileged attacker may be able to set a floating IP annotation to a pod even if the feature is not enabled. This may allow the attacker to intercept and reroute traffic to their compromised pod.	5.5	More Details
CVE-2022-29779	Nginx NJS v0.7.2 was discovered to contain a segmentation violation in the function njs_value_own_enumerate at src/njs_value.c.	5.5	More Details
CVE-2022-30747	PendingIntent hijacking vulnerability in Smart Things prior to 1.7.85.25 allows local attackers to access files without permission via implicit Intent.	5.5	More Details
CVE-2022-29780	Nginx NJS v0.7.2 was discovered to contain a segmentation violation in the function njs_array_prototype_sort at src/njs_array.c.	5.5	More Details
CVE-2021-43512	An issue was discovered in FlightRadar24 v8.9.0, v8.10.0, v8.10.2, v8.10.3, v8.10.4 for Android, allows attackers to cause unspecified consequences due to being able to decompile a local application and extract their API keys.	5.5	More Details
CVE-2022-30503	Nginx NJS v0.7.2 was discovered to contain a segmentation violation in the function njs_set_number at src/njs_value.h.	5.5	More Details
CVE-2021-42202	An issue was discovered in swftools through 20201222. A NULL pointer dereference exists in the function swf_DeleteFilter() located in swffilter.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2022-21749	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06511058; Issue ID: ALPS06511058.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30732	Exposure of Sensitive Information vulnerability in Samsung Account prior to version 13.2.00.6 allows attacker to access sensitive information via onActivityResult.	5.5	More Details
CVE-2022-21748	In telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS06511030; Issue ID: ALPS06511030.	5.5	More Details
CVE-2021-42200	An issue was discovered in swftools through 20201222. A NULL pointer dereference exists in the function main() located in swfdump.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2021-42198	An issue was discovered in swftools through 20201222. A NULL pointer dereference exists in the function swf_GetBits() located in rfxswf.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2022-31783	Liblouis 3.21.0 has an out-of-bounds write in compileRule in compileTranslationTable.c, as demonstrated by lou_trace.	5.5	More Details
CVE-2022-32202	In libjpeg 1.63, there is a NULL pointer dereference in LineBuffer::FetchRegion in linebuffer.cpp.	5.5	More Details
CVE-2021-42196	An issue was discovered in swftools through 20201222. A NULL pointer dereference exists in the function traits_parse() located in abc.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2022-32201	In libjpeg 1.63, there is a NULL pointer dereference in Component::SubXOf in component.hpp.	5.5	More Details
CVE-2022-29734	A cross-site scripting (XSS) vulnerability in ICT Protege GX/WX v2.08 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter.	5.4	More Details
CVE-2022-29770	XXL-Job v2.3.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability via /xxl-job-admin/jobinfo.	5.4	More Details
CVE-2021-38221	bbs-go <= 3.3.0 including Custom Edition is vulnerable to stored XSS.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29628	A cross-site scripting (XSS) vulnerability in /omps/seller of Online Market Place Site v1.0 allows attackers to execute arbitrary web cripts or HTML via a crafted payload injected into the Page parameter.	5.4	More Details
CVE-2022-29648	A cross-site scripting (XSS) vulnerability in Jfinal CMS v5.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted X-Forwarded-For request.	5.4	More Details
CVE-2022-2022	Cross-site Scripting (XSS) - Stored in GitHub repository nocodb/nocodb prior to 0.91.7.	5.4	More Details
CVE-2022-28051	The "Add category" functionality inside the "Global Keywords" menu in "SeedDMS" version 6.0.18 and 5.1.25, is prone to stored XSS which allows an attacker to inject malicious javascript code.	5.4	More Details
CVE-2022-1944	When the feature is configured, improper authorization in the Interactive Web Terminal in GitLab CE/EE affecting all versions from 11.3 prior to 14.9.5, 14.10 prior to 14.10.4, and 15.0 prior to 15.0.1 allows users with the Developer role to open terminals on other Developers' running jobs	5.4	More Details
CVE-2022-30429	Multiple cross-site scripting (XSS) vulnerabilities in Neos CMS allow attackers with the editor role or higher to inject arbitrary script or HTML code using the editor function, the deletion of assets, or a workspace title. The vulnerabilities were found in versions 3.3.29 and 8.0.1 and could also be present in all intermediate versions.	5.4	More Details
CVE-2022-26497	BigBlueButton Greenlight 2.11.1 allows XSS. A threat actor could have a username containing a JavaScript payload. The payload gets executed in the browser of the victim in the "Share room access" dialog if the victim has shared access to the particular room with the attacker previously.	5.4	More Details
CVE-2022-26976	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a license file upload mechanism. Lack of input sanitization in the upload mechanism is leads to reflected XSS.	5.4	More Details
CVE-2022-26973	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a license file upload mechanism. By tweaking the license file name, the returned error message exposes internal directory path details.	5.3	More Details
CVE-2022-32265	qDecoder before 12.1.0 does not ensure that the percent character is followed by two hex digits for URL decoding.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27779	libcurl wrongly allows cookies to be set for Top Level Domains (TLDs) if thehost name is provided with a trailing dot.curl can be told to receive and send cookies. curl's "cookie engine" can bebuilt with or without [Public Suffix List](https://publicsuffix.org/)awareness. If PSL support not provided, a more rudimentary check exists to atleast prevent cookies from being set on TLDs. This check was broken if thehost name in the URL uses a trailing dot.This can allow arbitrary sites to set cookies that then would get sent to adifferent and unrelated site or domain.	5.3	More Details
CVE-2022-29235	BigBlueButton is an open source web conferencing system. Starting in version 2.2 and prior to versions 2.3.18 and 2.4-rc-6, an attacker who is able to obtain the meeting identifier for a meeting on a server can find information related to an external video being shared, like the current timestamp and play/pause. The problem has been patched in versions 2.3.18 and 2.4-rc-6 by modifying the stream to send the data only for users in the meeting. There are currently no known workarounds.	5.3	More Details
CVE-2022-26971	Barco Control Room Management Suite web application, which is part of TransForm N before 3.14, is exposing a license file upload mechanism. This upload can be executed without authentication.	5.3	More Details
CVE-2022-29784	PublicCMS V4.0.202204.a and below contains an information leak via the component /views/directive/sys/SysConfigDataDirective.java.	5.3	More Details
CVE-2022-31485	An unauthenticated attacker can send a specially crafted packets to update the “notes” section of the home page of the web interface. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.29.	5.3	More Details
CVE-2022-30736	Improper privilege management vulnerability in Samsung Account prior to 13.2.00.6 allows attackers to get the data of contact and gallery without permission.	5.3	More Details
CVE-2021-39947	In specific circumstances, trace file buffers in GitLab Runner versions up to 14.3.4, 14.4 to 14.4.2, and 14.5 to 14.5.2 would re-use the file descriptor 0 for multiple traces and mix the output of several jobs	5.3	More Details
CVE-2022-30743	Improper privilege management vulnerability in Samsung Account prior to 13.2.00.6 allows attackers to get the data of contact and gallery without permission.	5.3	More Details
CVE-2022-30731	Improper access control vulnerability in My Files prior to version 13.1.00.193 allows attackers to access arbitrary private files in My Files application.	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33504	Couchbase Server before 7.1.0 has Incorrect Access Control.	4.9	More Details
CVE-2021-27778	HCL Traveler is vulnerable to a cross-site scripting (XSS) caused by improper validation of the Name parameter for Approved Applications in the Traveler administration web pages. An attacker could exploit this vulnerability to execute a malicious script to access any cookies, session tokens, or other sensitive information retained by the browser and used with that site.	4.9	More Details
CVE-2022-30863	FUDForum 3.1.2 is vulnerable to Cross Site Scripting (XSS) via page_title param in Page Manager in the Admin Control Panel.	4.8	More Details
CVE-2022-30861	FUDforum 3.1.2 is vulnerable to Stored XSS via Forum Name field in Forum Manager Feature.	4.8	More Details
CVE-2022-28479	SeedDMS versions 6.0.18 and 5.1.25 and below are vulnerable to stored XSS. An attacker with admin privileges can inject the payload inside the "Role management" menu and then trigger the payload by loading the "Users management" menu	4.8	More Details
CVE-2021-36866	Authenticated (author or higher role) Stored Cross-Site Scripting (XSS) vulnerability in Fatcat Apps Easy Pricing Tables plugin <= 3.1.2 at WordPress.	4.8	More Details
CVE-2022-30482	Ecommerce-project-with-php-and-mysqli-Fruits-Bazar- 1.0 is vulnerable to Cross Site Scripting (XSS) in \admin\add_cata.php via the ctg_name parameters.	4.8	More Details
CVE-2020-6220	BI Launchpad and CMC in SAP Business Objects Business Intelligence Platform, versions 4.1, 4.2, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. Exploit is possible only when the bttoken in victim’s session is active.	4.7	More Details
CVE-2022-1716	Keep My Notes v1.80.147 allows an attacker with physical access to the victim's device to bypass the application's password/pin lock to access user data. This is possible due to lack of adequate security controls to prevent dynamic code manipulation.	4.6	More Details
CVE-2022-30730	Improper authorization in Samsung Pass prior to 1.0.00.33 allows physical attackers to acess account list without authentication.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21762	In apusys driver, there is a possible system 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: ALPS06477946; Issue ID: ALPS06477946.	4.4	More Details
CVE-2022-21746	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479698; Issue ID: ALPS06479698.	4.4	More Details
CVE-2022-21755	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06545464; Issue ID: ALPS06545464.	4.4	More Details
CVE-2022-21756	In WLAN driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06535950; Issue ID: ALPS06535950.	4.4	More Details
CVE-2022-21760	In apusys driver, there is a possible system 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: ALPS06479562; Issue ID: ALPS06479562.	4.4	More Details
CVE-2022-21761	In apusys driver, there is a possible system 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: ALPS06479532; Issue ID: ALPS06479532.	4.4	More Details
CVE-2022-23236	E-Series SANtricity OS Controller Software versions 11.40 through 11.70.2 store the LDAP BIND password in plaintext within a file accessible only to privileged users.	4.4	More Details
CVE-2022-21747	In imgsensor, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478078; Issue ID: ALPS06478078.	4.4	More Details
CVE-2020-36534	A vulnerability was found in easyii CMS. It has been classified as problematic. Affected is an unknown function of the file /admin/sign/out. The manipulation leads to cross site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29627	An insecure direct object reference (IDOR) in Online Market Place Site v1.0 allows attackers to modify products that are owned by other sellers.	4.3	More Details
CVE-2021-42892	In TOTOLINK EX1200T V4.1.2cu.5215, an attacker can start telnet without authorization because the default username and password exists in the firmware.	4.3	More Details
CVE-2022-1821	An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.8 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting from 15.0 before 15.0.1. It may be possible for a subgroup member to access the members list of their parent group.	4.3	More Details
CVE-2022-1982	Uncontrolled resource consumption in Mattermost version 6.6.0 and earlier allows an authenticated attacker to crash the server via a crafted SVG attachment on a post.	4.3	More Details
CVE-2022-29234	BigBlueButton is an open source web conferencing system. Starting in version 2.2 and prior to versions 2.3.18 and 2.4.1, an attacker could send messages to a locked chat within a grace period of 5s any lock setting in the meeting was changed. The attacker needs to be a participant in the meeting. Versions 2.3.18 and 2.4.1 contain a patch for this issue. There are currently no known workarounds.	4.3	More Details
CVE-2022-29236	BigBlueButton is an open source web conferencing system. Starting in version 2.2 and prior to versions 2.3.18 and 2.4-rc-6, an attacker can circumvent access restrictions for drawing on the whiteboard. The permission check is inadvertently skipped on the server, due to a previously introduced grace period. The attacker must be a meeting participant. The problem has been patched in versions 2.3.18 and 2.4-rc-6. There are currently no known workarounds.	4.3	More Details
CVE-2022-30738	Improper check in Loader in Samsung Internet prior to 17.0.1.69 allows attackers to spoof address bar via executing script.	4.3	More Details
CVE-2022-29731	An access control issue in ICT Protege GX/WX 2.08 allows attackers to leak SHA1 password hashes of other users.	4.3	More Details
CVE-2022-30115	Using its HSTS support, curl can be instructed to use HTTPS directly insteadof using an insecure clear-text HTTP step even when HTTP is provided in theURL. This mechanism could be bypassed if the host name in the given URL used atrailing dot while not using one when it built the HSTS cache. Or the otherway around - by having the trailing dot in the HSTS cache and *not* using thetrailing dot in the URL.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26905	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4.3	More Details
CVE-2021-36890	Cross-Site Request Forgery (CSRF) vulnerability in Social Share Buttons by Supsystic plugin <= 2.2.2 at WordPress.	4.3	More Details
CVE-2020-36532	A vulnerability has been found in Klapp App and classified as problematic. This vulnerability affects unknown code of the component Authorization. The manipulation leads to information disclosure (Credentials). The attack can be initiated remotely. It is recommended to upgrade the affected app.	4.3	More Details
CVE-2022-29233	BigBlueButton is an open source web conferencing system. In BigBlueButton starting with 2.2 but before 2.3.18 and 2.4-rc-1, an attacker can circumvent access controls to gain access to all breakout rooms of the meeting they are in. The permission checks rely on knowledge of internal ids rather than on verification of the role of the user. Versions 2.3.18 and 2.4-rc-1 contain a patch for this issue. There are currently no known workarounds.	4.3	More Details
CVE-2022-30740	Improper auto-fill algorithm in Samsung Internet prior to version 17.0.1.69 allows physical attackers to guess stored credit card numbers.	4.1	More Details
CVE-2022-30733	Sensitive information exposure in Sign-in log in Samsung Account prior to version 13.2.00.6 allows attackers to get an user email or phone number without permission.	4.0	More Details
CVE-2022-30745	Improper access control vulnerability in Quick Share prior to version 13.1.2.4 allows attacker to access internal files in Quick Share.	4.0	More Details
CVE-2022-30734	Sensitive information exposure in Sign-out log in Samsung Account prior to version 13.2.00.6 allows attackers to get an user email or phone number without permission.	4.0	More Details
CVE-2022-30739	Improper privilege management vulnerability in Samsung Account prior to 13.2.00.6 allows attackers to get an user email or phone number with a normal level permission.	4.0	More Details
CVE-2022-30725	Broadcasting Intent including the BluetoothDevice object without proper restriction of receivers in sendIntentSessionError function of Bluetooth prior to SMR Jun-2022 Release 1 leaks MAC address of the connected Bluetooth device.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30724	Broadcasting Intent including the BluetoothDevice object without proper restriction of receivers in sendIntentSessionCompleted function of Bluetooth prior to SMR Jun-2022 Release 1 leaks MAC address of the connected Bluetooth device.	4.0	More Details
CVE-2022-30723	Broadcasting Intent including the BluetoothDevice object without proper restriction of receivers in activateVoiceRecognitionWithDevice function of Bluetooth prior to SMR Jun-2022 Release 1 leaks MAC address of the connected Bluetooth device.	4.0	More Details
CVE-2022-30737	Implicit Intent hijacking vulnerability in Samsung Account prior to version 13.2.00.6 allows attackers to get email ID.	4.0	More Details
CVE-2022-30717	Improper caller check in AR Emoji prior to SMR Jun-2022 Release 1 allows untrusted applications to use some camera functions via deeplink.	4.0	More Details
CVE-2022-30716	Unprotected broadcast in sendIntentForToastDumpLog in DisplayToast prior to SMR Jun-2022 Release 1 allows untrusted applications to access toast message information from device.	4.0	More Details
CVE-2022-30715	Improper access control vulnerability in DofViewer prior to SMR Jun-2022 Release 1 allows attackers to control floating system alert window.	4.0	More Details
CVE-2022-30748	Unprotected dynamic receiver in Samsung Members prior to version 4.2.005 allows attacker to launch arbitrary activity.	4.0	More Details
CVE-2022-22556	Dell PowerStore contains an Uncontrolled Resource Consumption Vulnerability in PowerStore User Interface. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the Denial of Service.	3.7	More Details
CVE-2020-36533	A vulnerability was found in Klapp App and classified as problematic. This issue affects some unknown processing of the JSON Web Token Handler. The manipulation leads to weak authentication. The attack may be initiated remotely.	3.7	More Details
CVE-2020-36527	A vulnerability, which was classified as problematic, has been found in Server Status. This issue affects some unknown processing of the component HTTP Status/SMTP Status. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1979	A vulnerability was found in SourceCodester Product Show Room Site 1.0. It has been declared as problematic. This vulnerability affects p=contact. The manipulation of the Message textbox with the input <script>alert(1)</script> leads to cross site scripting. The attack can be initiated remotely but requires authentication. Exploit details have been disclosed to the public.	3.5	More Details
CVE-2020-36526	A vulnerability classified as problematic was found in Countdown Timer. This vulnerability affects unknown code of the component Macro Handler. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2020-36525	A vulnerability classified as problematic has been found in Linking. This affects an unknown part of the component New Windows Macro. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2020-36524	A vulnerability was found in Refined Toolkit. It has been rated as problematic. Affected by this issue is some unknown functionality of the component UI-Image/UI-Button. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2020-36523	A vulnerability was found in PlantUML 6.43. It has been declared as problematic. Affected by this vulnerability is the component Database Information Macro. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2022-1991	A vulnerability classified as problematic has been found in Fast Food Ordering System 1.0. Affected is the file Master.php of the Master List. The manipulation of the argument Description with the input foo "><img src="" onerror="alert(document.cookie)"> leads to cross site scripting. It is possible to launch the attack remotely but it requires authentication. Exploit details have been disclosed to the public.	3.5	More Details
CVE-2022-30741	Sensitive information exposure vulnerability in SimChangeAlertManger of Find My Mobile prior to 7.2.24.12 allows local attackers with log access permission to get sim card information through device log.	3.3	More Details
CVE-2022-32296	The Linux kernel before 5.17.9 allows TCP servers to identify clients by observing what source ports are used. This occurs because of use of Algorithm 4 ("Double-Hash Port Selection Algorithm") of RFC 6056.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30742	Sensitive information exposure vulnerability in FmmExtraOperation of Find My Mobile prior to 7.2.24.12 allows local attackers with log access permissio to get sim card information through device log.	3.3	More Details
CVE-2022-30729	Implicit Intent hijacking vulnerability in Settings prior to SMR Jun-2022 Release 1 allows attackers to get Wi-Fi SSID and password via a malicious QR code scanner.	3.3	More Details
CVE-2022-30749	Improper access control vulnerability in Smart Things prior to 1.7.85.25 allows local attackers to add arbitrary smart devices by bypassing login activity.	3.3	More Details
CVE-2022-1783	An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.3 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting from 15.0 before 15.0.1. It may be possible for malicious group maintainers to add new members to a project within their group, through the REST API, even after their group owner enabled a setting to prevent members from being added to projects within that group.	2.7	More Details
CVE-2022-31025	Discourse is an open source platform for community discussion. Prior to version 2.8.4 on the `stable` branch and 2.9.0beta5 on the `beta` and `tests-passed` branches, inviting users on sites that use single sign-on could bypass the `must_approve_users` check and invites by staff are always approved automatically. The issue is patched in Discourse version 2.8.4 on the `stable` branch and version `2.9.0.beta5` on the `beta` and `tests-passed` branches. As a workaround, disable invites or increase `min_trust_level_to_allow_invite` to reduce the attack surface to more trusted users.	2.6	More Details
CVE-2022-30720	Improper input validation check logic vulnerability in libsmkvextractor prior to SMR Jun-2022 Release 1 allows attackers to trigger crash.	2.5	More Details
CVE-2022-30721	Improper input validation check logic vulnerability in libsmkvextractor prior to SMR Jun-2022 Release 1 allows attackers to trigger crash.	2.5	More Details
CVE-2022-30719	Improper input validation check logic vulnerability in libsmkvextractor prior to SMR Jun-2022 Release 1 allows attackers to trigger crash.	2.5	More Details
CVE-2022-30709	Improper input validation check logic vulnerability in SECRIL prior to SMR Jun-2022 Release 1 allows attackers to trigger crash.	2.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1980	A vulnerability was found in SourceCodester Product Show Room Site 1.0. It has been rated as problematic. This issue affects the file /admin/?page=system_info/contact_info. The manipulation of the textbox Telephone with the input <script>alert(1)</script> leads to cross site scripting. The attack may be initiated remotely but requires authentication. Exploit details have been disclosed to the public.	2.4	More Details
CVE-2022-31000	solidus_backend is the admin interface for the Solidus e-commerce framework. Versions prior to 3.1.6, 3.0.6, and 2.11.16 contain a cross-site request forgery (CSRF) vulnerability. The vulnerability allows attackers to change the state of an order's adjustments if they hold its number, and the execution happens on a store administrator's computer. Users should upgrade to solidus_backend 3.1.6, 3.0.6, or 2.11.16 to receive a patch.	2.3	More Details
CVE-2022-28794	Sensitive information exposure in low-battery dumpstate log prior to SMR Jun-2022 Release 1 allows local attackers to get SIM card information.	2.2	More Details
CVE-2022-30728	Information exposure vulnerability in ScanPool prior to SMR Jun-2022 Release 1 allows local attackers to get MAC address information.	1.9	More Details
CVE-2022-30714	Information exposure vulnerability in SemIWCMonitor prior to SMR Jun-2022 Release 1 allows local attackers to get MAC address information.	1.9	More Details
CVE-2021-3676	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-2022-1966	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-32250. Reason: This candidate is a duplicate of CVE-2022-32250. Notes: All CVE users should reference CVE-2022-32250 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2021-4014	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-2022-1550	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31279	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