SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 15 February 2023

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-2023-24482	A vulnerability has been identified in COMOS V10.2 (All versions), COMOS V10.3.3.1 (All versions < V10.3.3.1.45), COMOS V10.3.3.2 (All versions < V10.3.3.2.33), COMOS V10.3.3.3 (All versions < V10.3.3.3.9), COMOS V10.3.3.4 (All versions < V10.3.3.4.6), COMOS V10.4.0.0 (All versions < V10.4.0.0.31), COMOS V10.4.1.0 (All versions < V10.4.1.0.32), COMOS V10.4.2.0 (All versions < V10.4.2.0.25). Cache validation service in COMOS is vulnerable to Structured Exception Handler (SEH) based buffer overflow. This could allow an attacker to execute arbitrary code on the target system or cause denial of service condition.	10.0	More Details
CVE-2023-21803	Windows iSCSI Discovery Service Remote Code Execution Vulnerability	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4557	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Group Arge Energy and Control Systems Smartpower Web allows SQL Injection.This issue affects Smartpower Web: before 23.01.01.	9.8	More Details
CVE-2023-23162	Art Gallery Management System Project v1.0 was discovered to contain a SQL injection vulnerability via the cid parameter at product.php.	9.8	More Details
CVE-2023-23163	Art Gallery Management System Project v1.0 was discovered to contain a SQL injection vulnerability via the editid parameter.	9.8	More Details
CVE-2022-25729	Memory corruption in modem due to improper length check while copying into memory	9.8	More Details
CVE-2023-24160	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the admuser parameter in the setPasswordCfg function.	9.8	More Details
CVE-2022-33279	Memory corruption due to stack based buffer overflow in WLAN having invalid WNM frame length.	9.8	More Details
CVE-2022-40514	Memory corruption due to buffer copy without checking the size of input in WLAN Firmware while processing CCKM IE in reassoc response frame.	9.8	More Details
CVE-2022-45088	Improper Input Validation vulnerability in Group Arge Energy and Control Systems Smartpower Web allows PHP Local File Inclusion.This issue affects Smartpower Web: before 23.01.01.	9.8	More Details
CVE-2022-48322	NETGEAR Nighthawk WiFi Mesh systems and routers are affected by a stack-based buffer overflow vulnerability. This affects MR60 before 1.1.7.132, MS60 before 1.1.7.132, R6900P before 1.3.3.154, R7000P before 1.3.3.154, R7960P before 1.4.4.94, and R8000P before 1.4.4.94.	9.8	More Details
CVE-2022-47034	A type juggling vulnerability in the component /auth/fn.php of PlaySMS v1.4.5 and earlier allows attackers to bypass authentication.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48323	Sunlogin Sunflower Simplified (aka Sunflower Simple and Personal) 1.0.1.43315 is vulnerable to a path traversal issue. A remote and unauthenticated attacker can execute arbitrary programs on the victim host by sending a crafted HTTP request, as demonstrated by /check?cmd=ping../ followed by the pathname of the powershell.exe program.	9.8	More Details
CVE-2022-40022	Microchip Technology (Microsemi) SyncServer S650 was discovered to contain a command injection vulnerability.	9.8	More Details
CVE-2022-4445	The FL3R FeelBox WordPress plugin through 8.1 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection.	9.8	More Details
CVE-2023-24159	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the admpass parameter in the setPasswordCfg function.	9.8	More Details
CVE-2023-25717	Ruckus Wireless Admin through 10.4 allows Remote Code Execution via an unauthenticated HTTP GET Request, as demonstrated by a /forms/doLogin?login_username=admin&password=password$(curl substring.	9.8	More Details
CVE-2023-25718	In ConnectWise Control through 22.9.10032 (formerly known as ScreenConnect), after an executable file is signed, additional instructions can be added without invalidating the signature, such as instructions that result in offering the end user a (different) attacker-controlled executable file. It is plausible that the end user may allow the download and execution of this file to proceed. There are ConnectWise Control configuration options that add mitigations. NOTE: this may overlap CVE-2023-25719. NOTE: the vendor's position is that this purported vulnerability represents a "fundamental lack of understanding of Authenticode code signing behavior."	9.8	More Details
CVE-2023-24084	ChiKoi v1.0 was discovered to contain a SQL injection vulnerability via the load_file function.	9.8	More Details
CVE-2023-0777	Authentication Bypass by Primary Weakness in GitHub repository modoboa/modoboa prior to 2.0.4.	9.8	More Details
CVE-2023-24161	TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the webWlanIdx parameter in the setWebWlanIdx function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24352	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the webpage parameter at /goform/formWPS.	9.8	More Details
CVE-2023-24351	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the FILECODE parameter at /goform/formLogin.	9.8	More Details
CVE-2023-21716	Microsoft Word Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-21692	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-0744	Improper Access Control in GitHub repository answerdev/answer prior to 1.0.4.	9.8	More Details
CVE-2022-43764	Insufficient validation of input parameters when changing configuration on Tbase server in B&R APROL versions < R 4.2-07 could result in buffer overflow. This may lead to Denial-of-Service conditions or execution of arbitrary code.	9.8	More Details
CVE-2022-45526	SQL Injection vulnerability in Future-Depth Institutional Management Website (IMS) 1.0, allows attackers to execute arbitrary commands via the ad parameter to /admin_area/login_transfer.php.	9.8	More Details
CVE-2022-45527	File upload vulnerability in Future-Depth Institutional Management Website (IMS) 1.0, allows unauthorized attackers to directly upload malicious files to the courseimg directory.	9.8	More Details
CVE-2022-45982	thinkphp 6.0.0~6.0.13 and 6.1.0~6.1.1 contains a deserialization vulnerability. This vulnerability allows attackers to execute arbitrary code via a crafted payload.	9.8	More Details
CVE-2023-24646	An arbitrary file upload vulnerability in the component /fos/admin/ajax.php of Food Ordering System v2.0 allows attackers to execute arbitrary code via a crafted PHP file.	9.8	More Details
CVE-2023-21690	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43550	A command injection vulnerability exists in Jitsi before commit 8aa7be58522f4264078d54752aae5483bfd854b2 when launching browsers on Windows which could allow an attacker to insert an arbitrary URL which opens up the opportunity to remote execution.	9.8	More Details
CVE-2022-45699	Command injection in the administration interface in APSystems ECU-R version 5203 allows a remote unauthenticated attacker to execute arbitrary commands as root using the timezone parameter.	9.8	More Details
CVE-2023-21689	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-24348	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the curTime parameter at /goform/formSetACLFilter.	9.8	More Details
CVE-2023-24349	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the curTime parameter at /goform/formSetRoute.	9.8	More Details
CVE-2023-24350	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the config.smtp_email_subject parameter at /goform/formSetEmail.	9.8	More Details
CVE-2023-25168	Wings is Pterodactyl's server control plane. This vulnerability can be used to delete files and directories recursively on the host system. This vulnerability can be combined with `GHSA-p8r3-83r8-jwj5` to overwrite files on the host system. In order to use this exploit, an attacker must have an existing "server" allocated and controlled by Wings. This vulnerability has been resolved in version `v1.11.4` of Wings, and has been back-ported to the 1.7 release series in `v1.7.4`. Anyone running `v1.11.x` should upgrade to `v1.11.4` and anyone running `v1.7.x` should upgrade to `v1.7.4`. There are no known workarounds for this issue.	9.6	More Details
CVE-2022-43761	Missing authentication when creating and managing the B&R APROL database in versions < R 4.2-07 allows reading and changing the system configuration.	9.4	More Details
CVE-2022-33232	Memory corruption due to buffer copy without checking size of input while running memory sharing tests with large scattered memory.	9.3	More Details
CVE-2023-24188	ureport v2.2.9 was discovered to contain a directory traversal vulnerability via the deletion function which allows for arbitrary files to be deleted.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23551	Control By Web X-600M devices run Lua scripts and are vulnerable to code injection, which could allow an attacker to remotely execute arbitrary code.	9.1	More Details
CVE-2022-45766	Hardcoded credentials in Global Facilities Management Software (GFMS) Version 3 software distributed by Key Systems Management permits remote attackers to impact availability, confidentiality, accessibility and dependability of electronic key boxes.	9.1	More Details
CVE-2023-25725	HAProxy before 2.7.3 may allow a bypass of access control because HTTP/1 headers are inadvertently lost in some situations, aka "request smuggling." The HTTP header parsers in HAProxy may accept empty header field names, which could be used to truncate the list of HTTP headers and thus make some headers disappear after being parsed and processed for HTTP/1.0 and HTTP/1.1. For HTTP/2 and HTTP/3, the impact is limited because the headers disappear before being parsed and processed, as if they had not been sent by the client. The fixed versions are 2.7.3, 2.6.9, 2.5.12, 2.4.22, 2.2.29, and 2.0.31.	9.1	More Details
CVE-2022-43501	KASAGO TCP/IP stack provided by Zuken Elmic generates ISNs(Initial Sequence Number) for TCP connections from an insufficiently random source. An attacker may be able to determine the ISN of the current or future TCP connections and either hijack existing ones or spoof future ones.	9.1	More Details
CVE-2022-48290	The phone-PC collaboration module has a logic bypass vulnerability. Successful exploitation of this vulnerability may affect data confidentiality and integrity.	9.1	More Details
CVE-2023-0741	Cross-site Scripting (XSS) - DOM in GitHub repository answerdev/answer prior to 1.0.4.	9.0	More Details
CVE-2023-0743	Cross-site Scripting (XSS) - Generic in GitHub repository answerdev/answer prior to 1.0.4.	9.0	More Details
CVE-2023-0742	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.4.	9.0	More Details
CVE-2023-0740	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.4.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-0098	The Simple URLs WordPress plugin before 115 does not escape some parameters before using them in various SQL statements used by AJAX actions available by any authenticated users, leading to a SQL injection exploitable by low privilege users such as subscriber.	8.8	More Details
CVE-2023-0080	The Customer Reviews for WooCommerce WordPress plugin before 5.16.0 does not validate one of its shortcode attribute, which could allow users with a contributor role and above to include arbitrary files via a traversal attack. This could also allow them to read non PHP files and retrieve their content. RCE could also be achieved if the attacker manage to upload a malicious image containing PHP code, and then include it via the affected attribute, on a default WP install, authors could easily achieve that given that they have the upload_file capability.	8.8	More Details
CVE-2023-24343	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the curTime parameter at /goform/formSchedule.	8.8	More Details
CVE-2023-21717	Microsoft SharePoint Server Elevation of Privilege Vulnerability	8.8	More Details
CVE-2023-0260	The WP Review Slider WordPress plugin before 12.2 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as subscriber.	8.8	More Details
CVE-2023-0259	The WP Google Review Slider WordPress plugin before 11.8 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as subscriber.	8.8	More Details
CVE-2023-0771	SQL Injection in GitHub repository ampache/ampache prior to 5.5.7,develop.	8.8	More Details
CVE-2022-3568	The ImageMagick Engine plugin for WordPress is vulnerable to deserialization of untrusted input via the 'cli_path' parameter in versions up to, and including 1.7.5. This makes it possible for unauthenticated users to call files using a PHAR wrapper, granted they can trick a site administrator into performing an action such as clicking on a link, that will deserialize and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0255	The Enable Media Replace WordPress plugin before 4.0.2 does not prevent authors from uploading arbitrary files to the site, which may allow them to upload PHP shells on affected sites.	8.8	More Details
CVE-2023-0220	The Pinpoint Booking System WordPress plugin before 2.9.9.2.9 does not validate and escape one of its shortcode attributes before using it in a SQL statement, which could allow any authenticated users, such as subscriber to perform SQL Injection attacks.	8.8	More Details
CVE-2023-24323	Mojoportal v2.7 was discovered to contain an authenticated XML external entity (XXE) injection vulnerability.	8.8	More Details
CVE-2023-25149	TimescaleDB, an open-source time-series SQL database, has a privilege escalation vulnerability in versions 2.8.0 through 2.9.2. During installation, TimescaleDB creates a telemetry job that is runs as the installation user. The queries run as part of the telemetry data collection were not run with a locked down `search_path`, allowing malicious users to create functions that would be executed by the telemetry job, leading to privilege escalation. In order to be able to take advantage of this vulnerability, a user would need to be able to create objects in a database and then get a superuser to install TimescaleDB into their database. When TimescaleDB is installed as trusted extension, non-superusers can install the extension without help from a superuser. Version 2.9.3 fixes this issue. As a mitigation, the `search_path` of the user running the telemetry job can be locked down to not include schemas writable by other users. The vulnerability is not exploitable on instances in Timescale Cloud and Managed Service for TimescaleDB due to additional security provisions in place on those platforms.	8.8	More Details
CVE-2023-23912	A vulnerability, found in EdgeRouters Version 2.0.9-hotfix.5 and earlier and UniFi Security Gateways (USG) Version 4.4.56 and earlier with their DHCPv6 prefix delegation set to dhcpv6-stateless or dhcpv6-stateful, allows a malicious actor directly connected to the WAN interface of an affected device to create a remote code execution vulnerability.	8.8	More Details
CVE-2023-22794	A vulnerability in ActiveRecord <6.0.6.1, v6.1.7.1 and v7.0.4.1 related to the sanitization of comments. If malicious user input is passed to either the `annotate` query method, the `optimizer_hints` query method, or through the QueryLogs interface which automatically adds annotations, it may be sent to the database withinsufficient sanitization and be able to inject SQL outside of the comment.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22375	Cross-site request forgery (CSRF) vulnerability in Wired/Wireless LAN Pan/Tilt Network Camera CS-WMV02G all versions allows a remote unauthenticated attacker to hijack the authentication and conduct arbitrary operations by having a logged-in user to view a malicious page. NOTE: This vulnerability only affects products that are no longer supported by the developer.	8.8	More Details
CVE-2022-45725	Improper Input Validation in Comfast router CF-WR6110N V2.3.1 allows a remote attacker on the same network to execute arbitrary code on the target via an HTTP POST request	8.8	More Details
CVE-2023-24345	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the curTime parameter at /goform/formSetWanDhcpplus.	8.8	More Details
CVE-2023-21529	Microsoft Exchange Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-21684	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-21685	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-21686	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-21705	Microsoft SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-43440	Uncontrolled Search Path Element in Checkmk Agent in Tribe29 Checkmk before 2.1.0p1, before 2.0.0p25 and before 1.6.0p29 on a Checkmk server allows the site user to escalate privileges via a manipulated unixcat executable	8.8	More Details
CVE-2023-21799	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-0759	Privilege Chaining in GitHub repository cockpit-hq/cockpit prior to 2.3.8.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21706	Microsoft Exchange Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-22953	In ExpressionEngine before 7.2.6, remote code execution can be achieved by an authenticated Control Panel user.	8.8	More Details
CVE-2023-21798	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-21797	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-21707	Microsoft Exchange Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-24344	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the webpage parameter at /goform/formWlanGuestSetup.	8.8	More Details
CVE-2023-0261	The WP TripAdvisor Review Slider WordPress plugin before 10.8 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as subscriber.	8.8	More Details
CVE-2023-24346	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the wan_connected parameter at /goform/formEasySetupWizard3.	8.8	More Details
CVE-2022-34448	PowerPath Management Appliance with versions 3.3 & 3.2*, 3.1 & 3.0* contains a Cross-site Request Forgery vulnerability. An unauthenticated non-privileged user could potentially exploit the issue and perform any privileged state-changing actions.	8.8	More Details
CVE-2022-45089	Improper Input Validation vulnerability in Group Arge Energy and Control Systems Smartpower Web allows SQL Injection.This issue affects Smartpower Web: before 23.01.01.	8.8	More Details
CVE-2022-45090	Improper Input Validation vulnerability in Group Arge Energy and Control Systems Smartpower Web allows SQL Injection.This issue affects Smartpower Web: before 23.01.01.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24523	An attacker authenticated as a non-admin user with local access to a server port assigned to the SAP Host Agent (Start Service) - versions 7.21, 7.22, can submit a crafted ConfigureOutsideDiscovery request with an operating system command which will be executed with administrator privileges. The OS command can read or modify any user or system data and can make the system unavailable.	8.8	More Details
CVE-2023-24347	D-Link N300 WI-FI Router DIR-605L v2.13B01 was discovered to contain a stack overflow via the webpage parameter at /goform/formSetWanDhcpplus.	8.8	More Details
CVE-2023-25240	An improper SameSite Attribute vulnerability in pimCore v10.5.15 allows attackers to execute arbitrary code.	8.8	More Details
CVE-2023-25719	ConnectWise Control before 22.9.10032 (formerly known as ScreenConnect) fails to validate user-supplied parameters such as the Bin/ConnectWiseControl.Client.exe h parameter. This results in reflected data and injection of malicious code into a downloaded executable. The executable can be used to execute malicious queries or as a denial-of-service vector. NOTE: this CVE Record is only about the parameters, such as the h parameter (this CVE Record is not about the separate issue of signed executable files that are supposed to have unique configurations across customers' installations).	8.8	More Details
CVE-2022-45104	Dell Unisphere for PowerMax vApp, VASA Provider vApp, and Solution Enabler vApp version 9.2.3.x contain a command execution vulnerability. A low privileged remote attacker could potentially exploit this vulnerability, leading to execute arbitrary commands on the underlying system.	8.8	More Details
CVE-2023-21713	Microsoft SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-46649	Acemanager in ALEOS before version 4.16 allows a user with valid credentials to manipulate the IP logging operation to execute arbitrary shell commands on the device.	8.8	More Details
CVE-2023-0263	The WP Yelp Review Slider WordPress plugin before 7.1 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as subscriber.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34446	PowerPath Management Appliance with versions 3.3 & 3.2* contains Authorization Bypass vulnerability. An authenticated remote user with limited privileges (e.g., of role Monitoring) can exploit this issue and gain access to sensitive information, and modify the configuration.	8.8	More Details
CVE-2023-22629	An issue was discovered in TitanFTP through 1.94.1205. The move-file function has a path traversal vulnerability in the newPath parameter. An authenticated attacker can upload any file and then move it anywhere on the server's filesystem.	8.8	More Details
CVE-2023-0262	The WP Airbnb Review Slider WordPress plugin before 3.3 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as subscriber.	8.8	More Details
CVE-2022-46754	Wyse Management Suite 3.8 and below contain an improper access control vulnerability. A authenticated malicious admin user might access certain pro license features for which this admin is not authorized in order to configure user controlled external entities.	8.7	More Details
CVE-2023-21777	Azure App Service on Azure Stack Hub Elevation of Privilege Vulnerability	8.7	More Details
CVE-2023-22932	In Splunk Enterprise 9.0 versions before 9.0.4, a View allows for Cross-Site Scripting (XSS) through the error message in a Base64-encoded image. The vulnerability affects instances with Splunk Web enabled. It does not affect Splunk Enterprise versions below 9.0.	8.7	More Details
CVE-2022-41731	IBM Watson Knowledge Catalog on Cloud Pak for Data 4.5.0 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. IBM X-Force ID: 237402.	8.6	More Details
CVE-2023-25164	Tinacms is a Git-backed headless content management system with support for visual editing. Sites being built with @tinacms/cli >= 1.0.0 && < 1.0.9 which store sensitive values in the process.env variable are impacted. These values will be added in plaintext to the index.js file. If you're on a version prior to 1.0.0 this vulnerability does not affect you. If you are affected and your Tina-enabled website has sensitive credentials stored as environment variables (eg. Algolia API keys) you should rotate those keys immediately. This issue has been patched in @tinacms/cli@1.0.9. Users are advised to upgrade. There are no known workarounds for this issue.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23618	Git for Windows is the Windows port of the revision control system Git. Prior to Git for Windows version 2.39.2, when `gitk` is run on Windows, it potentially runs executables from the current directory inadvertently, which can be exploited with some social engineering to trick users into running untrusted code. A patch is available in version 2.39.2. As a workaround, avoid using `gitk` (or Git GUI's "Visualize History" functionality) in clones of untrusted repositories.	8.6	More Details
CVE-2023-0020	SAP BusinessObjects Business Intelligence platform - versions 420, 430, allows an authenticated attacker to access sensitive information which is otherwise restricted. On successful exploitation, there could be a high impact on confidentiality and limited impact on integrity of the application.	8.5	More Details
CVE-2023-21439	Improper input validation vulnerability in UwbDataTxStatusEvent prior to SMR Feb-2023 Release 1 allows attackers to launch certain activities.	8.5	More Details
CVE-2023-25152	Wings is Pterodactyl's server control plane. Affected versions are subject to a vulnerability which can be used to create new files and directory structures on the host system that previously did not exist, potentially allowing attackers to change their resource allocations, promote their containers to privileged mode, or potentially add ssh authorized keys to allow the attacker access to a remote shell on the target machine. In order to use this exploit, an attacker must have an existing "server" allocated and controlled by the Wings Daemon. This vulnerability has been resolved in version `v1.11.3` of the Wings Daemon, and has been back-ported to the 1.7 release series in `v1.7.3`. Anyone running `v1.11.x` should upgrade to `v1.11.3` and anyone running `v1.7.x` should upgrade to `v1.7.3`. There are no known workarounds for this vulnerability. ### Workarounds None at this time.	8.4	More Details
CVE-2023-0786	Cross-site Scripting (XSS) - Generic in GitHub repository thorsten/phpmyfaq prior to 3.1.11.	8.4	More Details
CVE-2022-33277	Memory corruption in modem due to buffer copy without checking size of input while receiving WMI command.	8.4	More Details
CVE-2023-24530	SAP BusinessObjects Business Intelligence Platform (CMC) - versions 420, 430, allows an authenticated admin user to upload malicious code that can be executed by the application over the network. On successful exploitation, attacker can perform operations that may completely compromise the application causing high impact on confidentiality, integrity and availability of the application.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33243	Memory corruption due to improper access control in Qualcomm IPC.	8.4	More Details
CVE-2023-0791	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.11.	8.3	More Details
CVE-2023-0794	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.11.	8.3	More Details
CVE-2023-23374	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	8.3	More Details
CVE-2022-33229	Information disclosure due to buffer over-read in Modem while using static array to process IPv4 packets.	8.2	More Details
CVE-2022-33271	Information disclosure due to buffer over-read in WLAN while parsing NMF frame.	8.2	More Details
CVE-2022-25738	Information disclosure in modem due to buffer over-red while performing checksum of packet received	8.2	More Details
CVE-2022-25732	Information disclosure in modem due to buffer over read in dns client due to missing length check	8.2	More Details
CVE-2022-25728	Information disclosure in modem due to buffer over-read while processing response from DNS server	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25559	DataHub is an open-source metadata platform. When not using authentication for the metadata service, which is the default configuration, the Metadata service (GMS) will use the X-DataHub-Actor HTTP header to infer the user the frontend is sending the request on behalf of. When the backends retrieves the header, its name is retrieved in a case-insensitive way. This case differential can be abused by an attacker to smuggle an X-DataHub-Actor header with different casing (eg: X-DATAHUB-ACTOR). This issue may lead to an authorization bypass by allowing any user to impersonate the system user account and perform any actions on its behalf. This vulnerability was discovered and reported by the GitHub Security lab and is tracked as GHSL-2022-079.	8.2	More Details
CVE-2023-25560	DataHub is an open-source metadata platform. The AuthServiceClient which is responsible for creation of new accounts, verifying credentials, resetting them or requesting access tokens, crafts multiple JSON strings using format strings with user-controlled data. This means that an attacker may be able to augment these JSON strings to be sent to the backend and that can potentially be abused by including new or colliding values. This issue may lead to an authentication bypass and the creation of system accounts, which effectively can lead to full system compromise. Users are advised to upgrade. There are no known workarounds for this vulnerability. This vulnerability was discovered and reported by the GitHub Security lab and is tracked as GHSL-2022-080.	8.2	More Details
CVE-2022-38657	An open redirect to malicious sites can occur when accessing the "Feedback" action on the manager page.	8.2	More Details
CVE-2023-21806	Power BI Report Server Spoofing Vulnerability	8.2	More Details
CVE-2023-0776	Baicells Nova 436Q, Nova 430E, Nova 430I, and Neutrino 430 LTE TDD eNodeB devices with firmware through QRTB 2.12.7 are vulnerable to remote shell code exploitation via HTTP command injections. Commands are executed using pre-login execution and executed with root permissions. The following methods below have been tested and validated by a 3rd party analyst and has been confirmed exploitable special thanks to Rustam Amin for providing the steps to reproduce.	8.1	More Details
CVE-2023-22935	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the ‘display.page.search.patterns.sensitivity’ search parameter lets a search bypass SPL safeguards for risky commands. The vulnerability requires a higher privileged user to initiate a request within their browser and only affects instances with Splunk Web enabled.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0789	Command Injection in GitHub repository thorsten/phpmyfaq prior to 3.1.11.	8.1	More Details
CVE-2023-0788	Code Injection in GitHub repository thorsten/phpmyfaq prior to 3.1.11.	8.1	More Details
CVE-2023-0787	Cross-site Scripting (XSS) - Generic in GitHub repository thorsten/phpmyfaq prior to 3.1.11.	8.1	More Details
CVE-2023-22939	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'map' search processing language (SPL) command lets a search bypass SPL safeguards for risky commands. The vulnerability requires a higher privileged user to initiate a request within their browser and only affects instances with Splunk Web enabled.	8.1	More Details
CVE-2023-24828	Onedev is a self-hosted Git Server with CI/CD and Kanban. In versions prior to 7.9.12 the algorithm used to generate access token and password reset keys was not cryptographically secure. Existing normal users (or everyone if it allows self-registration) may exploit this to elevate privilege to obtain administrator permission. This issue is has been addressed in version 7.9.12. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.1	More Details
CVE-2023-21778	Microsoft Dynamics Unified Service Desk Remote Code Execution Vulnerability	8.0	More Details
CVE-2023-22933	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, a View allows for Cross-Site Scripting (XSS) in an extensible mark-up language (XML) View through the 'layoutPanel' attribute in the 'module' tag'.	8.0	More Details
CVE-2023-24990	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19812)	7.8	More Details
CVE-2022-47977	A vulnerability has been identified in JT Open (All versions < V11.2.3.0), JT Utilities (All versions < V13.2.3.0). The affected application contains a memory corruption vulnerability while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24989	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19811)	7.8	More Details
CVE-2023-23376	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-24992	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19814)	7.8	More Details
CVE-2023-21822	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-24549	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected application is vulnerable to stack-based buffer while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2023-24987	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19809)	7.8	More Details
CVE-2023-24991	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19813)	7.8	More Details
CVE-2023-24994	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19816)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48077	Genymotion Desktop v3.3.2 was discovered to contain a DLL hijacking vulnerability that allows attackers to escalate privileges and execute arbitrary code via a crafted DLL.	7.8	More Details
CVE-2022-47936	A vulnerability has been identified in JT Open (All versions < V11.2.3.0), JT Utilities (All versions < V13.2.3.0), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170), Parasolid V35.1 (All versions < V35.1.150). The affected application contains a stack overflow vulnerability while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-0770	Stack-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.2.	7.8	More Details
CVE-2023-24993	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19815)	7.8	More Details
CVE-2023-24550	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected application is vulnerable to heap-based buffer while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2023-24995	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19817)	7.8	More Details
CVE-2022-31808	A vulnerability has been identified in SiPass integrated AC5102 (ACC-G2) (All versions < V2.85.44), SiPass integrated ACC-AP (All versions < V2.85.43). Affected devices improperly sanitize user input on the telnet command line interface. This could allow an authenticated user to escalate privileges by injecting arbitrary commands that are executed with root privileges.	7.8	More Details
CVE-2023-24996	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19818)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25140	A vulnerability has been identified in Parasolid V34.0 (All versions < V34.0.254), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170), Parasolid V35.1 (All versions < V35.1.150), Solid Edge SE2022 (All versions < V222.0MP12). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-23377	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21809	Microsoft Defender for Endpoint Security Feature Bypass Vulnerability	7.8	More Details
CVE-2023-24988	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19810)	7.8	More Details
CVE-2023-24554	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-25396	Privilege escalation in the MSI repair functionality in Caphyon Advanced Installer 20.0 and below allows attackers to access and manipulate system files.	7.8	More Details
CVE-2023-24556	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2022-34384	Dell SupportAssist Client Consumer (version 3.11.1 and prior), SupportAssist Client Commercial (version 3.2 and prior), Dell Command l Update, Dell Update, and Alienware Update versions before 4.5 contain a Local Privilege Escalation Vulnerability in the Advanced Driver Restore component. A local malicious user may potentially exploit this vulnerability, leading to privilege escalation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24557	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-24558	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-24559	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-24560	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to to execute code in the context of the current process.	7.8	More Details
CVE-2023-24561	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2023-24562	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2023-24563	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24564	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2022 (All versions), Solid Edge SE2023 (All versions < V223.0Update2). The affected application contains a memory corruption vulnerability while parsing specially crafted DWG files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19069)	7.8	More Details
CVE-2023-24581	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2022 (All versions), Solid Edge SE2023 (All versions < V223.0Update2). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted STP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19425)	7.8	More Details
CVE-2023-24978	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted SPP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19788)	7.8	More Details
CVE-2023-24979	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19789)	7.8	More Details
CVE-2023-24980	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19790)	7.8	More Details
CVE-2023-24981	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19791)	7.8	More Details
CVE-2023-21817	Windows Kerberos Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24553	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-24552	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected application contains an out of bounds read past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to to execute code in the context of the current process.	7.8	More Details
CVE-2023-24551	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected application is vulnerable to heap-based buffer underflow while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2023-21812	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-24982	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19804)	7.8	More Details
CVE-2023-24983	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19805)	7.8	More Details
CVE-2023-24984	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19806)	7.8	More Details
CVE-2023-24569	Dell Alienware Command Center versions 5.5.37.0 and prior contain an Improper Input validation vulnerability. A local authenticated malicious user could potentially send malicious input to a named pipe in order to elevate privileges on the system.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24985	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19807)	7.8	More Details
CVE-2023-24986	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19808)	7.8	More Details
CVE-2023-24555	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2023 (All versions < V223.0Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-21800	Windows Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-47361	In firewall service, there is a missing permission check. This could lead to local escalation of privilege with system execution privileges needed.	7.8	More Details
CVE-2023-21433	Improper access control vulnerability in Galaxy Store prior to version 4.5.49.8 allows local attackers to install applications from Galaxy Store.	7.8	More Details
CVE-2023-22360	Use-after free vulnerability exists in Screen Creator Advance 2 Ver.0.1.1.4 Build01 and earlier due to lack of error handling process even when an error was detected. Having a user of Screen Creator Advance 2 to open a specially crafted project file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-22353	Out-of-bound read vulnerability exists in Screen Creator Advance 2 Ver.0.1.1.4 Build01 and earlier because the end of data cannot be verified when processing control management information. Having a user of Screen Creator Advance 2 to open a specially crafted project file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-23378	Print 3D Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0249	Delta Electronics DIAScreen versions 1.2.1.23 and prior are vulnerable to out-of-bounds write, which may allow an attacker to remotely execute arbitrary code.	7.8	More Details
CVE-2023-0250	Delta Electronics DIAScreen versions 1.2.1.23 and prior are vulnerable to a stack-based buffer overflow, which could allow an attacker to remotely execute arbitrary code.	7.8	More Details
CVE-2023-21688	NT OS Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21808	.NET and Visual Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21815	Visual Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-22346	Out-of-bound read vulnerability exists in Screen Creator Advance 2 Ver.0.1.1.4 Build01 and earlier because the end of data cannot be verified when processing template information. Having a user of Screen Creator Advance 2 to open a specially crafted project file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-22345	Out-of-bound write vulnerability exists in Screen Creator Advance 2 Ver.0.1.1.4 Build01 and earlier due to lack of error handling process when out of specification errors are detected. Having a user of Screen Creator Advance 2 to open a specially crafted project file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-22350	Out-of-bound read vulnerability exists in Screen Creator Advance 2 Ver.0.1.1.4 Build01 and earlier because the end of data cannot be verified when processing parts management information. Having a user of Screen Creator Advance 2 to open a specially crafted project file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-21823	Windows Graphics Component Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22349	Out-of-bound read vulnerability exists in Screen Creator Advance 2 Ver.0.1.1.4 Build01 and earlier because the end of data cannot be verified when processing screen management information. Having a user of Screen Creator Advance 2 to open a specially crafted project file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-21704	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-0251	Delta Electronics DIAScreen versions 1.2.1.23 and prior are vulnerable to a buffer overflow through improper restrictions of operations within memory, which could allow an attacker to remotely execute arbitrary code.	7.8	More Details
CVE-2023-0760	Heap-based Buffer Overflow in GitHub repository gpac/gpac prior to V2.1.0-DEV.	7.8	More Details
CVE-2023-21718	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21528	Microsoft SQL Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-33233	Memory corruption due to configuration weakness in modem wile sending command to write protected files.	7.8	More Details
CVE-2023-24187	An XML External Entity (XXE) vulnerability in ureport v2.2.9 allows attackers to execute arbitrary code via uploading a crafted XML file to /ureport/designer/saveReportFile.	7.8	More Details
CVE-2023-0127	A command injection vulnerability in the firmware_update command, in the device's restricted telnet interface, allows an authenticated attacker to execute arbitrary commands as root.	7.8	More Details
CVE-2023-23379	Microsoft Defender for IoT Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38396	HP Factory Preinstalled Images on certain systems that shipped with Windows 10 versions 20H2 and earlier OS versions might allow escalation of privilege via execution of certain files outside the restricted path. This potential vulnerability was remediated starting with Windows 10 versions 21H2 on October 31, 2021.	7.8	More Details
CVE-2023-0817	Buffer Over-read in GitHub repository gpac/gpac prior to v2.3.0-DEV.	7.8	More Details
CVE-2023-23390	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21805	Windows MSHTML Platform Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21804	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21566	Visual Studio Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21802	Windows Media Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-22347	Out-of-bound read vulnerability exists in Screen Creator Advance 2 Ver.0.1.1.4 Build01 and earlier because the end of data cannot be verified when processing file structure information. Having a user of Screen Creator Advance 2 to open a specially crafted project file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-0819	Heap-based Buffer Overflow in GitHub repository gpac/gpac prior to v2.3.0-DEV.	7.8	More Details
CVE-2022-38777	An issue was discovered in the rollback feature of Elastic Endpoint Security for Windows, which could allow unprivileged users to elevate their privileges to those of the LocalSystem account.	7.8	More Details
CVE-2023-23381	Visual Studio Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33248	Memory corruption in User Identity Module due to integer overflow to buffer overflow when a segement is received via qmi http.	7.8	More Details
CVE-2022-45455	Local privilege escalation due to incomplete uninstallation cleanup. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40107, Acronis Agent (Windows) before build 30025, Acronis Cyber Protect 15 (Windows) before build 30984.	7.8	More Details
CVE-2023-21801	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-33934	Dell PowerScale OneFS, versions 8.2.x through 9.4.x contain multiple stored cross-site scripting vulnerabilities. A remote authenticated malicious user with high privileges may potentially exploit these vulnerabilities to store malicious HTML or JavaScript code through multiple affected fields.	7.7	More Details
CVE-2023-0790	Uncaught Exception in GitHub repository thorsten/phpmyfaq prior to 3.1.11.	7.6	More Details
CVE-2022-47648	An Improper Access Control vulnerability allows an attacker to access the control panel of the B420 without requiring any sort of authorization or authentication due to the IP based authorization. If an authorized user has accessed a publicly available B420 product using valid credentials, an insider attacker can gain access to the same panel without requiring any sort of authorization. The B420 module was already obsolete at the time this vulnerability was found (The End of Life announcement was made in 2013).	7.6	More Details
CVE-2022-33306	Transient DOS due to buffer over-read in WLAN while processing an incoming management frame with incorrectly filled IEs.	7.5	More Details
CVE-2022-34145	Transient DOS due to buffer over-read in WLAN Host while parsing frame information.	7.5	More Details
CVE-2023-21819	Windows Secure Channel Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34146	Transient DOS due to improper input validation in WLAN Host while parsing frame during defragmentation.	7.5	More Details
CVE-2022-40502	Transient DOS due to improper input validation in WLAN Host.	7.5	More Details
CVE-2023-25558	DataHub is an open-source metadata platform. When the DataHub frontend is configured to authenticate via SSO, it will leverage the pac4j library. The processing of the `id_token` is done in an unsafe manner which is not properly accounted for by the DataHub frontend. Specifically, if any of the id_token claims value start with the {#sb64} prefix, pac4j considers the value to be a serialized Java object and will deserialize it. This issue may lead to Remote Code Execution (RCE) in the worst case. Although a `RestrictedObjectInputStream` is in place, that puts some restriction on what classes can be deserialized, it still allows a broad range of java packages and potentially exploitable with different gadget chains. Users are advised to upgrade. There are no known workarounds. This vulnerability was discovered and reported by the GitHub Security lab and is tracked as GHSL-2022-086.	7.5	More Details
CVE-2022-40512	Transient DOS in WLAN Firmware due to buffer over-read while processing probe response or beacon.	7.5	More Details
CVE-2022-40513	Transient DOS due to uncontrolled resource consumption in WLAN firmware when peer is freed in non qos state.	7.5	More Details
CVE-2022-25735	Denial of service in modem due to missing null check while processing TCP or UDP packets from server	7.5	More Details
CVE-2022-25734	Denial of service in modem due to missing null check while processing IP packets with padding	7.5	More Details
CVE-2022-25733	Denial of service in modem due to null pointer dereference while processing DNS packets	7.5	More Details
CVE-2023-21553	Azure DevOps Server Remote Code Execution Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43765	B&R APROL versions < R 4.2-07 doesn't process correctly specially formatted data packages sent to port 55502/tcp, which may allow a network based attacker to cause an application Denial-of-Service.	7.5	More Details
CVE-2023-22854	The ccmweb component of Mitel MiContact Center Business server 9.2.2.0 through 9.4.1.0 could allow an unauthenticated attacker to download arbitrary files, due to insufficient restriction of URL parameters. A successful exploit could allow access to sensitive information.	7.5	More Details
CVE-2023-25577	Werkzeug is a comprehensive WSGI web application library. Prior to version 2.2.3, Werkzeug's multipart form data parser will parse an unlimited number of parts, including file parts. Parts can be a small amount of bytes, but each requires CPU time to parse and may use more memory as Python data. If a request can be made to an endpoint that accesses `request.data`, `request.form`, `request.files`, or `request.get_data(parse_form_data=False)`, it can cause unexpectedly high resource usage. This allows an attacker to cause a denial of service by sending crafted multipart data to an endpoint that will parse it. The amount of CPU time required can block worker processes from handling legitimate requests. The amount of RAM required can trigger an out of memory kill of the process. Unlimited file parts can use up memory and file handles. If many concurrent requests are sent continuously, this can exhaust or kill all available workers. Version 2.2.3 contains a patch for this issue.	7.5	More Details
CVE-2022-43763	Insufficient check of preconditions could lead to Denial of Service conditions when calling commands on the Tbase server of B&R APROL versions < R 4.2-07.	7.5	More Details
CVE-2022-43762	Lack of verification in B&R APROL Tbase server versions < R 4.2-07 may lead to memory leaks when receiving messages	7.5	More Details
CVE-2023-24647	Food Ordering System v2.0 was discovered to contain a SQL injection vulnerability via the email parameter.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25557	DataHub is an open-source metadata platform. The DataHub frontend acts as a proxy able to forward any REST or GraphQL requests to the backend. The goal of this proxy is to perform authentication if needed and forward HTTP requests to the DataHub Metadata Store (GMS). It has been discovered that the proxy does not adequately construct the URL when forwarding data to GMS, allowing external users to reroute requests from the DataHub Frontend to any arbitrary hosts. As a result attackers may be able to reroute a request from originating from the frontend proxy to any other server and return the result. This vulnerability was discovered and reported by the GitHub Security lab and is tracked as GHSL-2022-076.	7.5	More Details
CVE-2022-48288	The bundle management module lacks authentication and control mechanisms in some APIs. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2023-21818	Windows Secure Channel Denial of Service Vulnerability	7.5	More Details
CVE-2022-42438	IBM Cloud Pak for Multicloud Management Monitoring 2.0 and 2.3 allows users without admin roles access to admin functions by specifying direct URL paths. IBM X-Force ID: 238210.	7.5	More Details
CVE-2023-21444	Improper cryptographic implementation in Samsung Flow for PC 4.9.14.0 allows adjacent attackers to decrypt encrypted messages or inject commands.	7.5	More Details
CVE-2023-21443	Improper cryptographic implementation in Samsung Flow for Android prior to version 4.9.04 allows adjacent attackers to decrypt encrypted messages or inject commands.	7.5	More Details
CVE-2023-25565	GSS-NTLMSSP is a mechglue plugin for the GSSAPI library that implements NTLM authentication. Prior to version 1.2.0, an incorrect free when decoding target information can trigger a denial of service. The error condition incorrectly assumes the `cb` and `sh` buffers contain a copy of the data that needs to be freed. However, that is not the case. This vulnerability can be triggered via the main `gss_accept_sec_context` entry point. This will likely trigger an assertion failure in `free`, causing a denial-of-service. This issue is fixed in version 1.2.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25566	GSS-NTLMSSP is a mechglue plugin for the GSSAPI library that implements NTLM authentication. Prior to version 1.2.0, a memory leak can be triggered when parsing usernames which can trigger a denial-of-service. The domain portion of a username may be overridden causing an allocated memory area the size of the domain name to be leaked. An attacker can leak memory via the main `gss_accept_sec_context` entry point, potentially causing a denial-of-service. This issue is fixed in version 1.2.0.	7.5	More Details
CVE-2023-25567	GSS-NTLMSSP, a mechglue plugin for the GSSAPI library that implements NTLM authentication, has an out-of-bounds read when decoding target information prior to version 1.2.0. The length of the `av_pair` is not checked properly for two of the elements which can trigger an out-of-bound read. The out-of-bounds read can be triggered via the main `gss_accept_sec_context` entry point and could cause a denial-of-service if the memory is unmapped. The issue is fixed in version 1.2.0.	7.5	More Details
CVE-2022-45454	Sensitive information disclosure due to insecure folder permissions. The following products are affected: Acronis Agent (Windows) before build 30161, Acronis Cyber Protect 15 (Windows) before build 30984.	7.5	More Details
CVE-2023-22362	SUSHIRO App for Android outputs sensitive information to the log file, which may result in an attacker obtaining a credential information from the log file. Affected products/versions are as follows: SUSHIRO Ver.4.0.31, Thailand SUSHIRO Ver.1.0.0, Hong Kong SUSHIRO Ver.3.0.2, Singapore SUSHIRO Ver.2.0.0, and Taiwan SUSHIRO Ver.2.0.1	7.5	More Details
CVE-2023-21691	Microsoft Protected Extensible Authentication Protocol (PEAP) Information Disclosure Vulnerability	7.5	More Details
CVE-2023-21695	Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability	7.5	More Details
CVE-2023-21700	Windows iSCSI Discovery Service Denial of Service Vulnerability	7.5	More Details
CVE-2023-21701	Microsoft Protected Extensible Authentication Protocol (PEAP) Denial of Service Vulnerability	7.5	More Details
CVE-2023-21702	Windows iSCSI Service Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48302	The AMS module has a vulnerability of lacking permission verification in APIs.Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-48301	The bundle management module lacks permission verification in some APIs. Successful exploitation of this vulnerability may restore the pre-installed apps that have been uninstalled.	7.5	More Details
CVE-2022-48300	The WMS module lacks the authentication mechanism in some APIs. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-48299	The WMS module lacks the authentication mechanism in some APIs. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-48298	The geofencing kernel code does not verify the length of the input data. Successful exploitation of this vulnerability may cause out-of-bounds memory access.	7.5	More Details
CVE-2022-48297	The geofencing kernel code has a vulnerability of not verifying the length of the input data. Successful exploitation of this vulnerability may cause out-of-bounds memory access.	7.5	More Details
CVE-2022-48286	The multi-screen collaboration module has a privilege escalation vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-48295	The IHwAntiMalPlugin interface lacks permission verification. Successful exploitation of this vulnerability can lead to filling problems (batch installation of applications).	7.5	More Details
CVE-2022-48294	The IHwAttestationService interface has a defect in authentication. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-43460	Driver Distributor v2.2.3.1 and earlier contains a vulnerability where passwords are stored in a recoverable format. If an attacker obtains a configuration file of Driver Distributor, the encrypted administrator's credentials may be decrypted.	7.5	More Details
CVE-2022-48287	The HwContacts module has a logic bypass vulnerability. Successful exploitation of this vulnerability may affect data integrity.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0159	The Extensive VC Addons for WPBakery page builder WordPress plugin before 1.9.1 does not validate a parameter passed to the php extract function when loading templates, allowing an unauthenticated attacker to override the template path to read arbitrary files from the hosts file system. This may be escalated to RCE using PHP filter chains.	7.5	More Details
CVE-2022-44566	A denial of service vulnerability present in ActiveRecord's PostgreSQL adapter <7.0.4.1 and <6.1.7.1. When a value outside the range for a 64bit signed integer is provided to the PostgreSQL connection adapter, it will treat the target column type as numeric. Comparing integer values against numeric values can result in a slow sequential scan resulting in potential Denial of Service.	7.5	More Details
CVE-2022-44570	A denial of service vulnerability in the Range header parsing component of Rack >= 1.5.0. A Carefully crafted input can cause the Range header parsing component in Rack to take an unexpected amount of time, possibly resulting in a denial of service attack vector. Any applications that deal with Range requests (such as streaming applications, or applications that serve files) may be impacted.	7.5	More Details
CVE-2022-44571	There is a denial of service vulnerability in the Content-Disposition parsingcomponent of Rack fixed in 2.0.9.2, 2.1.4.2, 2.2.4.1, 3.0.0.1. This could allow an attacker to craft an input that can cause Content-Disposition header parsing in Rackto take an unexpected amount of time, possibly resulting in a denial ofservice attack vector. This header is used typically used in multipartparsing. Any applications that parse multipart posts using Rack (virtuallyall Rails applications) are impacted.	7.5	More Details
CVE-2023-21816	Windows Active Directory Domain Services API Denial of Service Vulnerability	7.5	More Details
CVE-2023-21813	Windows Secure Channel Denial of Service Vulnerability	7.5	More Details
CVE-2023-21811	Windows iSCSI Service Denial of Service Vulnerability	7.5	More Details
CVE-2022-48289	The bundle management module lacks authentication and control mechanisms in some APIs. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4450	The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data. If the function succeeds then the "name_out", "header" and "data" arguments are populated with pointers to buffers containing the relevant decoded data. The caller is responsible for freeing those buffers. It is possible to construct a PEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex() will return a failure code but will populate the header argument with a pointer to a buffer that has already been freed. If the caller also frees this buffer then a double free will occur. This will most likely lead to a crash. This could be exploited by an attacker who has the ability to supply malicious PEM files for parsing to achieve a denial of service attack. The functions PEM_read_bio() and PEM_read() are simple wrappers around PEM_read_bio_ex() and therefore these functions are also directly affected. These functions are also called indirectly by a number of other OpenSSL functions including PEM_X509_INFO_read_bio_ex() and SSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internal uses of these functions are not vulnerable because the caller does not free the header argument if PEM_read_bio_ex() returns a failure code. These locations include the PEM_read_bio_TYPE() functions as well as the decoders introduced in OpenSSL 3.0. The OpenSSL asn1parse command line application is also impacted by this issue.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0215	The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and smime command line applications are similarly affected.	7.5	More Details
CVE-2023-0216	An invalid pointer dereference on read can be triggered when an application tries to load malformed PKCS7 data with the d2i_PKCS7(), d2i_PKCS7_bio() or d2i_PKCS7_fp() functions. The result of the dereference is an application crash which could lead to a denial of service attack. The TLS implementation in OpenSSL does not call this function however third party applications might call these functions on untrusted data.	7.5	More Details
CVE-2023-0217	An invalid pointer dereference on read can be triggered when an application tries to check a malformed DSA public key by the EVP_PKEY_public_check() function. This will most likely lead to an application crash. This function can be called on public keys supplied from untrusted sources which could allow an attacker to cause a denial of service attack. The TLS implementation in OpenSSL does not call this function but applications might call the function if there are additional security requirements imposed by standards such as FIPS 140-3.	7.5	More Details
CVE-2023-23592	WALLIX Access Manager 3.x through 4.0.x allows a remote attacker to access sensitive information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21940	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute vulnerability in Johnson Controls System Configuration Tool (SCT) version 14 prior to 14.2.3 and version 15 prior to 15.0.3 could allow access to the cookie.	7.5	More Details
CVE-2022-21939	Sensitive Cookie Without 'HttpOnly' Flag vulnerability in Johnson Controls System Configuration Tool (SCT) version 14 prior to 14.2.3 and version 15 prior to 15.0.3 could allow access to the cookie.	7.5	More Details
CVE-2023-25141	Apache Sling JCR Base < 3.1.12 has a critical injection vulnerability when running on old JDK versions (JDK 1.8.191 or earlier) through utility functions in RepositoryAccessor. The functions getRepository and getRepositoryFromURL allow an application to access data stored in a remote location via JDNI and RMI. Users of Apache Sling JCR Base are recommended to upgrade to Apache Sling JCR Base 3.1.12 or later, or to run on a more recent JDK.	7.5	More Details
CVE-2023-0401	A NULL pointer can be dereferenced when signatures are being verified on PKCS7 signed or signedAndEnveloped data. In case the hash algorithm used for the signature is known to the OpenSSL library but the implementation of the hash algorithm is not available the digest initialization will fail. There is a missing check for the return value from the initialization function which later leads to invalid usage of the digest API most likely leading to a crash. The unavailability of an algorithm can be caused by using FIPS enabled configuration of providers or more commonly by not loading the legacy provider. PKCS7 data is processed by the SMIME library calls and also by the time stamp (TS) library calls. The TLS implementation in OpenSSL does not call these functions however third party applications would be affected if they call these functions to verify signatures on untrusted data.	7.5	More Details
CVE-2023-22799	A ReDoS based DoS vulnerability in the GlobalID <1.0.1 which could allow an attacker supplying a carefully crafted input can cause the regular expression engine to take an unexpected amount of time. All users running an affected release should either upgrade or use one of the workarounds immediately.	7.5	More Details
CVE-2021-46023	An Untrusted Pointer Dereference was discovered in function mrb_vm_exec in mruby before 3.1.0-rc. The vulnerability causes a segmentation fault and application crash.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25576	@fastify/multipart is a Fastify plugin to parse the multipart content-type. Prior to versions 7.4.1 and 6.0.1, @fastify/multipart may experience denial of service due to a number of situations in which an unlimited number of parts are accepted. This includes the multipart body parser accepting an unlimited number of file parts, the multipart body parser accepting an unlimited number of field parts, and the multipart body parser accepting an unlimited number of empty parts as field parts. This is fixed in v7.4.1 (for Fastify v4.x) and v6.0.1 (for Fastify v3.x). There are no known workarounds.	7.5	More Details
CVE-2023-22796	A regular expression based DoS vulnerability in Active Support <6.1.7.1 and <7.0.4.1. A specially crafted string passed to the underscore method can cause the regular expression engine to enter a state of catastrophic backtracking. This can cause the process to use large amounts of CPU and memory, leading to a possible DoS vulnerability.	7.5	More Details
CVE-2023-22795	A regular expression based DoS vulnerability in Action Dispatch <6.1.7.1 and <7.0.4.1 related to the If-None-Match header. A specially crafted HTTP If-None-Match header can cause the regular expression engine to enter a state of catastrophic backtracking, when on a version of Ruby below 3.2.0. This can cause the process to use large amounts of CPU and memory, leading to a possible DoS vulnerability All users running an affected release should either upgrade or use one of the workarounds immediately.	7.5	More Details
CVE-2023-25151	opentelemetry-go-contrib is a collection of extensions for OpenTelemetry-Go. The v0.38.0 release of `go.opentelemetry.io/contrib/instrumentation/net/http/otelhttp` uses the `httpconv.ServerRequest` function to annotate metric measurements for the `http.server.request_content_length`, `http.server.response_content_length`, and `http.server.duration` instruments. The `ServerRequest` function sets the `http.target` attribute value to be the whole request URI (including the query string)[^1]. The metric instruments do not "forget" previous measurement attributes when `cumulative` temporality is used, this means the cardinality of the measurements allocated is directly correlated with the unique URIs handled. If the query string is constantly random, this will result in a constant increase in memory allocation that can be used in a denial-of-service attack. This issue has been addressed in version 0.39.0. Users are advised to upgrade. There are no known workarounds for this issue.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22792	A regular expression based DoS vulnerability in Action Dispatch <6.0.6.1, < 6.1.7.1, and <7.0.4.1. Specially crafted cookies, in combination with a specially crafted X_FORWARDED_HOST header can cause the regular expression engine to enter a state of catastrophic backtracking. This can cause the process to use large amounts of CPU and memory, leading to a possible DoS vulnerability All users running an affected release should either upgrade or use one of the workarounds immediately.	7.5	More Details
CVE-2022-44572	A denial of service vulnerability in the multipart parsing component of Rack fixed in 2.0.9.2, 2.1.4.2, 2.2.4.1 and 3.0.0.1 could allow an attacker tocraft input that can cause RFC2183 multipart boundary parsing in Rack to take an unexpected amount of time, possibly resulting in a denial of service attack vector. Any applications that parse multipart posts using Rack (virtually all Rails applications) are impacted.	7.5	More Details
CVE-2023-22832	The ExtractCCDAAttributes Processor in Apache NiFi 1.2.0 through 1.19.1 does not restrict XML External Entity references. Flow configurations that include the ExtractCCDAAttributes Processor are vulnerable to malicious XML documents that contain Document Type Declarations with XML External Entity references. The resolution disables Document Type Declarations and disallows XML External Entity resolution in the ExtractCCDAAttributes Processor.	7.5	More Details
CVE-2023-0286	There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.	7.4	More Details
CVE-2023-21820	Windows Distributed File System (DFS) Remote Code Execution Vulnerability	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21441	Insufficient Verification of Data Authenticity vulnerability in Routine prior to versions 2.6.30.6 in Android Q(10), 3.1.21.10 in Android R(11) and 3.5.2.23 in Android S(12) allows local attacker to access protected files via unused code.	7.4	More Details
CVE-2023-0784	A vulnerability classified as critical has been found in SourceCodester Best Online News Portal 1.0. Affected is an unknown function of the component Login Page. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-220644.	7.3	More Details
CVE-2023-22934	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'pivot' search processing language (SPL) command lets a search bypass SPL safeguards for risky commands using a saved search job. The vulnerability requires an authenticated user to craft the saved job and a higher privileged user to initiate a request within their browser.	7.3	More Details
CVE-2023-21715	Microsoft Publisher Security Feature Bypass Vulnerability	7.3	More Details
CVE-2022-33280	Memory corruption due to access of uninitialized pointer in Bluetooth HOST while processing the AVRCP packet.	7.3	More Details
CVE-2023-0774	A vulnerability has been found in SourceCodester Medical Certificate Generator App 1.0 and classified as critical. This vulnerability affects unknown code of the file action.php. The manipulation of the argument lastname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-220558 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2023-21568	Microsoft SQL Server Integration Service (VS extension) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-21420	Use of Externally-Controlled Format String vulnerabilities in STST TA prior to SMR Jan-2023 Release 1 allows arbitrary code execution.	7.3	More Details
CVE-2022-4546	The Mapwiz WordPress plugin through 1.0.1 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24684	ChurchCRM v4.5.3 and below was discovered to contain a SQL injection vulnerability via the EID parameter at GetText.php.	7.2	More Details
CVE-2023-24685	ChurchCRM v4.5.3 and below was discovered to contain a SQL injection vulnerability via the Event parameter under the Event Attendance reports module.	7.2	More Details
CVE-2022-34447	PowerPath Management Appliance with versions 3.3 & 3.2*, 3.1 & 3.0* contains OS Command Injection vulnerability. An authenticated remote attacker with administrative privileges could potentially exploit the issue and execute commands on the system as the root user.	7.2	More Details
CVE-2023-21710	Microsoft Exchange Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2023-0782	A vulnerability was found in Tenda AC23 16.03.07.45 and classified as critical. Affected by this issue is the function formSetSysToolDDNS/formGetSysToolDDNS of the file /bin/httpd. The manipulation leads to out-of-bounds write. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-220640.	7.2	More Details
CVE-2023-20076	A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system.	7.2	More Details
CVE-2023-0575	External Control of Critical State Data, Improper Control of Generation of Code ('Code Injection') vulnerability in YugaByte, Inc. Yugabyte DB on Windows, Linux, MacOS, iOS (DevopsBase.Java:execCommand, TableManager.Java:runCommand modules) allows API Manipulation, Privilege Abuse. This vulnerability is associated with program files backup.Py. This issue affects Yugabyte DB: Lesser then 2.2.0.0	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22743	Git for Windows is the Windows port of the revision control system Git. Prior to Git for Windows version 2.39.2, by carefully crafting DLL and putting into a subdirectory of a specific name living next to the Git for Windows installer, Windows can be tricked into side-loading said DLL. This potentially allows users with local write access to place malicious payloads in a location where automated upgrades might run the Git for Windows installer with elevation. Version 2.39.2 contains a patch for this issue. Some workarounds are available. Never leave untrusted files in the Downloads folder or its sub-folders before executing the Git for Windows installer, or move the installer into a different directory before executing it.	7.2	More Details
CVE-2023-0793	Weak Password Requirements in GitHub repository thorsten/phpmyfaq prior to 3.1.11.	7.1	More Details
CVE-2022-4745	The WP Customer Area WordPress plugin before 8.1.4 does not have CSRF checks when performing some actions such as chmod, mkdir and copy, which could allow attackers to make a logged-in admin perform them and create arbitrary folders, copy file for example.	7.1	More Details
CVE-2022-34388	Dell SupportAssist for Home PCs (version 3.11.4 and prior) and SupportAssist for Business PCs (version 3.2.0 and prior) contain information disclosure vulnerability. A local malicious user with low privileges could exploit this vulnerability to view and modify sensitive information in the database of the affected application.	7.1	More Details
CVE-2023-21564	Azure DevOps Server Cross-Site Scripting Vulnerability	7.1	More Details
CVE-2022-43779	A potential Time-of-Check to Time-of-Use (TOCTOU) vulnerability has been identified in certain HP PC products using AMI UEFI Firmware (system BIOS) which might allow arbitrary code execution, denial of service, and information disclosure. AMI has released updates to mitigate the potential vulnerability.	7.0	More Details
CVE-2022-34397	Dell Unisphere for PowerMax vApp, VASA Provider vApp, and Solution Enabler vApp version 10.0.0.5 and below contains an authorization bypass vulnerability, allowing users to perform actions in which they are not authorized.	6.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25562	DataHub is an open-source metadata platform. In versions of DataHub prior to 0.8.45 Session cookies are only cleared on new sign-in events and not on logout events. Any authentication checks using the `AuthUtils.hasValidSessionCookie()` method could be bypassed by using a cookie from a logged out session, as a result any logged out session cookie may be accepted as valid and therefore lead to an authentication bypass to the system. Users are advised to upgrade. There are no known workarounds for this issue. This vulnerability was discovered and reported by the GitHub Security lab and is tracked as GHSL-2022-083.	6.9	More Details
CVE-2022-41564	The Hawk Console component of TIBCO Software Inc.'s TIBCO Hawk and TIBCO Operational Intelligence Hawk RedTail contains a vulnerability that will return the EMS transport password and EMS SSL password to a privileged user. Affected releases are TIBCO Software Inc.'s TIBCO Hawk: versions 6.1.0 through 6.2.1 and TIBCO Operational Intelligence Hawk RedTail: versions 7.0.0 through 7.2.0.	6.8	More Details
CVE-2023-0804	LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in tools/tiffcrop.c:3609, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 33aee127.	6.8	More Details
CVE-2023-25571	Backstage is an open platform for building developer portals. `@backstage/catalog-model` prior to version 1.2.0, `@backstage/core-components` prior to 0.12.4, and `@backstage/plugin-catalog-backend` prior to 1.7.2 are affected by a cross-site scripting vulnerability. This vulnerability allows a malicious actor with access to add or modify content in an instance of the Backstage software catalog to inject script URLs in the entities stored in the catalog. If users of the catalog then click on said URLs, that can lead to an XSS attack. This vulnerability has been patched in both the frontend and backend implementations. The default `Link` component from `@backstage/core-components` version 1.2.0 and greater will now reject `javascript:` URLs, and there is a global override of `window.open` to do the same. In addition, the catalog model v0.12.4 and greater as well as the catalog backend v1.7.2 and greater now has additional validation built in that prevents `javascript:` URLs in known annotations. As a workaround, the general practice of limiting access to modifying catalog content and requiring code reviews greatly help mitigate this vulnerability.	6.8	More Details
CVE-2023-0739	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') in GitHub repository answerdev/answer prior to 1.0.4.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0574	Server-Side Request Forgery (SSRF), Improperly Controlled Modification of Dynamically-Determined Object Attributes, Improper Restriction of Excessive Authentication Attempts vulnerability in YugaByte, Inc. Yugabyte Managed allows Accessing Functionality Not Properly Constrained by ACLs, Communication Channel Manipulation, Authentication Abuse.This issue affects Yugabyte Managed: from 2.0.0.0 through 2.13.0.0	6.8	More Details
CVE-2022-24410	Dell BIOS contains an information exposure vulnerability. An unauthenticated local attacker with physical access to the system and knowledge of the system configuration could potentially exploit this vulnerability to read system information via debug interfaces.	6.8	More Details
CVE-2022-33221	Information disclosure in Trusted Execution Environment due to buffer over-read while processing metadata verification requests.	6.8	More Details
CVE-2023-0799	LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3701, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit afaabc3e.	6.8	More Details
CVE-2023-0798	LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3400, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit afaabc3e.	6.8	More Details
CVE-2022-46677	Wyse Management Suite 3.8 and below contain an improper access control vulnerability with which an custom group admin can create a subgroup under a group for which the admin is not authorized.	6.8	More Details
CVE-2023-21694	Windows Fax Service Remote Code Execution Vulnerability	6.8	More Details
CVE-2023-0802	LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in tools/tiffcrop.c:3724, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 33aee127.	6.8	More Details
CVE-2023-0801	LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in libtiff/tif_unix.c:368, invoked by tools/tiffcrop.c:2903 and tools/tiffcrop.c:6778, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 33aee127.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0800	LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in tools/tiffcrop.c:3502, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 33aee127.	6.8	More Details
CVE-2023-0795	LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3488, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit afaabc3e.	6.8	More Details
CVE-2023-0796	LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3592, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit afaabc3e.	6.8	More Details
CVE-2023-0797	LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in libtiff/tif_unix.c:368, invoked by tools/tiffcrop.c:2903 and tools/tiffcrop.c:6921, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit afaabc3e.	6.8	More Details
CVE-2023-0803	LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in tools/tiffcrop.c:3516, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 33aee127.	6.8	More Details
CVE-2023-0745	The High Availability functionality of Yugabyte Anywhere can be abused to write arbitrary files through the backup upload endpoint by using path traversal characters. This vulnerability is associated with program files PlatformReplicationManager.Java. This issue affects YugabyteDB Anywhere: from 2.0.0.0 through 2.13.0.0	6.7	More Details
CVE-2022-34454	Dell PowerScale OneFS, versions 8.2.x-9.3.x, contain a heap-based buffer overflow. A local privileged malicious user could potentially exploit this vulnerability, leading to system takeover. This impacts compliance mode clusters.	6.7	More Details
CVE-2023-21451	A Stack-based overflow vulnerability in IpcRxEmbmsSessionList in SECRIL prior to Android S(12) allows attacker to cause memory corruptions.	6.7	More Details
CVE-2022-47341	In engineermode services, there is a missing permission check. This could lead to local escalation of privilege with system execution privileges needed.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47339	In cmd services, there is a OS command injection issue due to missing permission check. This could lead to local escalation of privilege with system execution privileges needed.	6.7	More Details
CVE-2022-34450	PowerPath Management Appliance with version 3.3 contains Privilege Escalation vulnerability. An authenticated admin user could potentially exploit this issue and gain unrestricted control/code execution on the system as root.	6.7	More Details
CVE-2022-35868	A vulnerability has been identified in TIA Multiuser Server V14 (All versions), TIA Multiuser Server V15 (All versions < V15.1 Update 8), TIA Project-Server (All versions < V1.1), TIA Project-Server V16 (All versions), TIA Project-Server V17 (All versions < V17 Update 6). Affected applications contain an untrusted search path vulnerability that could allow an attacker to escalate privileges, when tricking a legitimate user to start the service from an attacker controlled path.	6.7	More Details
CVE-2022-33246	Memory corruption in Audio due to use of out-of-range pointer offset while Initiating a voice call session from user space with invalid session id.	6.7	More Details
CVE-2022-33225	Memory corruption due to use after free in trusted application environment.	6.7	More Details
CVE-2022-3411	A lack of length validation in GitLab CE/EE affecting all versions from 12.4 before 15.6.7, 15.7 before 15.7.6, and 15.8 before 15.8.1 allows an authenticated attacker to create a large Issue description via GraphQL which, when repeatedly requested, saturates CPU usage.	6.5	More Details
CVE-2023-0814	The Profile Builder – User Profile & User Registration Forms plugin for WordPress is vulnerable to sensitive information disclosure via the [user_meta] shortcode in versions up to, and including 3.9.0. This is due to insufficient restriction on sensitive user meta values that can be called via that shortcode. This makes it possible for authenticated attackers, with subscriber-level permissions, and above to retrieve sensitive user meta that can be used to gain access to a high privileged user account. This does require the Usermeta shortcode be enabled to be exploited.	6.5	More Details
CVE-2023-23382	Azure Machine Learning Compute Instance Information Disclosure Vulnerability	6.5	More Details
CVE-2023-21807	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0792	Code Injection in GitHub repository thorsten/phpmyfaq prior to 3.1.11.	6.5	More Details
CVE-2023-0024	SAP Solution Manager (BSP Application) - version 720, allows an authenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information or craft a payload which may restrict access to the desired resources, resulting in Cross-Site Scripting vulnerability.	6.5	More Details
CVE-2023-21721	Microsoft OneNote Elevation of Privilege Vulnerability	6.5	More Details
CVE-2023-24524	SAP S/4 HANA Map Treasury Correspondence Format Data does not perform necessary authorization check for an authenticated user, resulting in escalation of privileges. This could allow an attacker to delete the data with a high impact to availability.	6.5	More Details
CVE-2023-0025	SAP Solution Manager (BSP Application) - version 720, allows an authenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information or craft a payload which may restrict access to the desired resources.	6.5	More Details
CVE-2023-23855	SAP Solution Manager - version 720, allows an authenticated attacker to redirect users to a malicious site due to insufficient URL validation. A successful attack could lead an attacker to read or modify the information or expose the user to a phishing attack. As a result, it has a low impact to confidentiality, integrity and availability.	6.5	More Details
CVE-2023-22941	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, an improperly-formatted ‘INGEST_EVAL’ parameter in a Field Transformation crashes the Splunk daemon (splunkd).	6.5	More Details
CVE-2023-21703	Azure Data Box Gateway Remote Code Execution Vulnerability	6.5	More Details
CVE-2023-24528	SAP Fiori apps for Travel Management in SAP ERP (My Travel Requests) - version 600, allows an authenticated attacker to exploit a certain misconfigured application endpoint to view sensitive data. This endpoint is normally exposed over the network and successful exploitation can lead to exposure of data like travel documents.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45962	Open Solutions for Education, Inc openSIS Community Edition v8.0 and earlier is vulnerable to SQL Injection via CalendarModal.php.	6.5	More Details
CVE-2023-21572	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	6.5	More Details
CVE-2022-25937	Versions of the package glance before 3.0.9 are vulnerable to Directory Traversal that allows users to read files outside the public root directory. This is related to but distinct from the vulnerability reported in [CVE-2018-3715](https://security.snyk.io/vuln/npm:glance:20180129).	6.5	More Details
CVE-2023-25564	GSS-NTLMSSP is a mechglue plugin for the GSSAPI library that implements NTLM authentication. Prior to version 1.2.0, memory corruption can be triggered when decoding UTF16 strings. The variable `outlen` was not initialized and could cause writing a zero to an arbitrary place in memory if `ntlm_str_convert()` were to fail, which would leave `outlen` uninitialized. This can lead to a denial of service if the write hits unmapped memory or randomly corrupts a byte in the application memory space. This vulnerability can trigger an out-of-bounds write, leading to memory corruption. This vulnerability can be triggered via the main `gss_accept_sec_context` entry point. This issue is fixed in version 1.2.0.	6.5	More Details
CVE-2023-0019	In SAP GRC (Process Control) - versions GRCFND_A V1200, GRCFND_A V8100, GRCPINW V1100_700, GRCPINW V1100_731, GRCPINW V1200_750, remote-enabled function module in the proprietary SAP solution enables an authenticated attacker with minimal privileges to access all the confidential data stored in the database. Successful exploitation of this vulnerability can expose user credentials from client-specific tables of the database, leading to high impact on confidentiality.	6.5	More Details
CVE-2022-40480	Nordic Semiconductor, Microchip Technology NRF5340-DK DT100112 was discovered to contain an issue which allows attackers to cause a Denial of Service (DoS) via a crafted ConReq packet.	6.5	More Details
CVE-2023-25167	Discourse is an open source discussion platform. In affected versions a malicious user can cause a regular expression denial of service using a carefully crafted git URL. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. Users are advised to upgrade. There are no known workarounds for this issue.	6.5	More Details
CVE-2022-45191	An issue was discovered on Microchip RN4870 1.43 devices. An attacker within BLE radio range can cause a denial of service by sending a pair confirm message with wrong values.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45085	Server-Side Request Forgery (SSRF) vulnerability in Group Arge Energy and Control Systems Smartpower Web allows : Server Side Request Forgery.This issue affects Smartpower Web: before 23.01.01.	6.5	More Details
CVE-2022-43869	IBM Spectrum Scale (5.1.0.0 through 5.1.2.8 and 5.1.3.0 through 5.1.5.1) and IBM Elastic Storage System (6.1.0.0 through 6.1.2.4 and 6.1.3.0 through 6.1.4.1) could allow an authenticated user to cause a denial of service through the GUI using a format string attack. IBM X-Force ID: 239539.	6.5	More Details
CVE-2023-0003	A file disclosure vulnerability in the Palo Alto Networks Cortex XSOAR server software enables an authenticated user with access to the web interface to read local files from the server.	6.5	More Details
CVE-2022-48292	The Bluetooth module has an out-of-memory (OOM) vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	6.5	More Details
CVE-2022-48293	The Bluetooth module has an OOM vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	6.5	More Details
CVE-2022-34366	Dell SupportAssist for Home PCs (version 3.11.2 and prior) contain Overly Permissive Cross-domain Whitelist vulnerability. An authenticated non-admin user could potentially exploit the issue and obtain sensitive information.	6.5	More Details
CVE-2022-45192	An issue was discovered on Microchip RN4870 1.43 devices. An attacker within BLE radio range can cause a denial of service by sending a cleartext encryption pause request.	6.5	More Details
CVE-2022-38778	A flaw (CVE-2022-38900) was discovered in one of Kibana's third party dependencies, that could allow an authenticated user to perform a request that crashes the Kibana server process.	6.5	More Details
CVE-2022-34404	Dell System Update, version 2.0.0 and earlier, contains an Improper Certificate Validation in data parser module. A local attacker with high privileges could potentially exploit this vulnerability, leading to credential theft and/or denial of service.	6.5	More Details
CVE-2023-0751	When GELI reads a key file from standard input, it does not reuse the key file to initialize multiple providers at once resulting in the second and subsequent devices silently using a NULL key as the user key file. If a user only uses a key file without a user passphrase, the master key is encrypted with an empty key file allowing trivial recovery of the master key.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0661	Improper access control in Devolutions Server allows an authenticated user to access unauthorized sensitive data.	6.5	More Details
CVE-2022-4138	A Cross Site Request Forgery issue has been discovered in GitLab CE/EE affecting all versions before 15.6.7, all versions starting from 15.7 before 15.7.6, and all versions starting from 15.8 before 15.8.1. An attacker could take over a project if an Owner or Maintainer uploads a file to a malicious project.	6.4	More Details
CVE-2023-0748	Open Redirect in GitHub repository btcpayserver/btcpayserver prior to 1.7.6.	6.4	More Details
CVE-2022-34387	Dell SupportAssist for Home PCs (version 3.11.4 and prior) and SupportAssist for Business PCs (version 3.2.0 and prior) contain a privilege escalation vulnerability. A local authenticated malicious user could potentially exploit this vulnerability to elevate privileges and gain total control of the system.	6.4	More Details
CVE-2022-3089	Echelon SmartServer 2.2 with i.LON Vision 2.2 stores cleartext credentials in a file, which could allow an attacker to obtain cleartext usernames and passwords of the SmartServer. If the attacker obtains the file, then the credentials could be used to control the web user interface and file transfer protocol (FTP) server.	6.3	More Details
CVE-2023-0781	A vulnerability was found in SourceCodester Canteen Management System 1.0. It has been declared as critical. This vulnerability affects the function query of the file removeOrder.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-220624.	6.3	More Details
CVE-2023-0758	A vulnerability was found in glorylion JFinalOA 1.0.2 and classified as critical. This issue affects some unknown processing of the file src/main/java/com/pointlion/mvc/common/model/SysOrg.java. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-220469 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-10077	A vulnerability was found in webbuilders-group silverstripe-kapost-bridge 0.3.3. It has been declared as critical. Affected by this vulnerability is the function index/getPreview of the file code/control/KapostService.php. The manipulation leads to sql injection. The attack can be launched remotely. Upgrading to version 0.4.0 is able to address this issue. The patch is named 2e14b0fd0ea35034f90890f364b130fb4645ff35. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-220471.	6.3	More Details
CVE-2023-0830	A vulnerability classified as critical has been found in EasyNAS 1.1.0. Affected is the function system of the file /backup.pl. The manipulation leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. VDB-220950 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-25163	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All versions of Argo CD starting with v2.6.0-rc1 have an output sanitization bug which leaks repository access credentials in error messages. These error messages are visible to the user, and they are logged. The error message is visible when a user attempts to create or update an Application via the Argo CD API (and therefor the UI or CLI). The user must have `applications, create` or `applications, update` RBAC access to reach the code which may produce the error. The user is not guaranteed to be able to trigger the error message. They may attempt to spam the API with requests to trigger a rate limit error from the upstream repository. If the user has `repositories, update` access, they may edit an existing repository to introduce a URL typo or otherwise force an error message. But if they have that level of access, they are probably intended to have access to the credentials anyway. A patch for this vulnerability has been released in version 2.6.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.3	More Details
CVE-2023-22940	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, aliases of the ‘collect’ search processing language (SPL) command, including ‘summaryindex’, ‘sumindex’, ‘stash’,’ mcollect’, and ‘meventcollect’, were not designated as safeguarded commands. The commands could potentially allow for the exposing of data to a summary index that unprivileged users could access. The vulnerability requires a higher privileged user to initiate a request within their browser, and only affects instances with Splunk Web enabled.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22936	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the 'search_listener' parameter in a search allows for a blind server-side request forgery (SSRF) by an authenticated user. The initiator of the request cannot see the response without the presence of an additional vulnerability within the environment.	6.3	More Details
CVE-2023-23946	Git, a revision control system, is vulnerable to path traversal prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8. By feeding a crafted input to `git apply`, a path outside the working tree can be overwritten as the user who is running `git apply`. A fix has been prepared and will appear in v2.39.2, v2.38.4, v2.37.6, v2.36.5, v2.35.7, v2.34.7, v2.33.7, v2.32.6, v2.31.7, and v2.30.8. As a workaround, use `git apply --stat` to inspect a patch before applying; avoid applying one that creates a symbolic link and then creates a file beyond the symbolic link.	6.2	More Details
CVE-2023-21440	Improper access control vulnerability in WindowManagerService prior to SMR Feb-2023 Release 1 allows attackers to take a screen capture.	6.2	More Details
CVE-2023-21697	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability	6.2	More Details
CVE-2023-23948	The ownCloud Android app allows ownCloud users to access, share, and edit files and folders. Version 2.21.1 of the ownCloud Android app is vulnerable to SQL injection in `FileContentProvider.kt`. This issue can lead to information disclosure. Two databases, `filelist` and `owncloud_database`, are affected. In version 3.0, the `filelist` database was deprecated. However, injections affecting `owncloud_database` remain relevant as of version 3.0.	6.2	More Details
CVE-2023-21446	Improper input validation in MyFiles prior to version 12.2.09 in Android R(11), 13.1.03.501 in Android S(12) and 14.1.00.422 in Android T(13) allows local attacker to access data of MyFiles.	6.2	More Details
CVE-2023-21434	Improper input validation vulnerability in Galaxy Store prior to version 4.5.49.8 allows local attackers to execute JavaScript by launching a web page.	6.2	More Details
CVE-2023-24322	A reflected cross-site scripting (XSS) vulnerability in the FileDialog.aspx component of mojoPortal v2.7.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the ed and tbi parameters.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25614	SAP NetWeaver AS ABAP (BSP Framework) application - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allow an unauthenticated attacker to inject the code that can be executed by the application over the network. On successful exploitation it can gain access to the sensitive information which leads to a limited impact on the confidentiality and the integrity of the application.	6.1	More Details
CVE-2023-24529	Due to lack of proper input validation, BSP application (CRM_BSP_FRAME) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, allow malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a Reflected Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to hijack a user session, read and modify some sensitive information.	6.1	More Details
CVE-2023-23161	A reflected cross-site scripting (XSS) vulnerability in Art Gallery Management System Project v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the artname parameter under ART TYPE option in the navigation bar.	6.1	More Details
CVE-2022-44261	Avery Dennison Monarch Printer M9855 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2023-24522	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (Business Server Pages) - versions 700, 701, 702, 731, 740, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application.	6.1	More Details
CVE-2023-23860	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a link, which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack.	6.1	More Details
CVE-2023-23859	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to craft a malicious link, which when clicked by an unsuspecting user, can be used to read or modify some sensitive information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23858	Due to insufficient input validation, SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, allows an unauthenticated attacker to send a crafted URL to a user, and by clicking the URL, the tricked user accesses SAP and might be directed with the response to somewhere out-side SAP and enter sensitive data. This could cause a limited impact on confidentiality and integrity of the application.	6.1	More Details
CVE-2023-23853	An unauthenticated attacker in AP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, can craft a link which when clicked by an unsuspecting user can be used to redirect a user to a malicious site which could read or modify some sensitive information or expose the victim to a phishing attack. Vulnerability has no direct impact on availability.	6.1	More Details
CVE-2023-22797	An open redirect vulnerability is fixed in Rails 7.0.4.1 with the new protection against open redirects from calling redirect_to with untrusted user input. In prior versions the developer was fully responsible for only providing trusted input. However the check introduced could allow an attacker to bypass with a carefully crafted URL resulting in an open redirect vulnerability.	6.1	More Details
CVE-2023-25241	bgERP v22.31 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the Search parameter.	6.1	More Details
CVE-2022-48110	CKSource CKEditor 5 35.4.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the Full Featured CKEditor5 widget. NOTE: the vendor's position is that this is not a vulnerability. The CKEditor 5 documentation discusses that it is the responsibility of an integrator (who is adding CKEditor 5 functionality to a website) to choose the correct security settings for their use case. Also, safe default values are established (e.g., config.htmlEmbed.showPreviews is false).	6.1	More Details
CVE-2023-23852	SAP Solution Manager (System Monitoring) - version 720, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2023-22376	Reflected cross-site scripting vulnerability in Wired/Wireless LAN Pan/Tilt Network Camera CS-WMV02G all versions allows a remote unauthenticated attacker to inject arbitrary script to inject an arbitrary script. NOTE: This vulnerability only affects products that are no longer supported by the developer.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22798	Prior to commit 51867e0d15a6d7f80d5b714fd0e9976b9c160bb0, https://github.com/brave/adblock-lists removed redirect interceptors on some websites like Facebook in which the redirect interceptor may have been there for security purposes. This could potentially cause open redirects on these websites. Brave's redirect interceptor removal feature is known as "debouncing" and is intended to remove unnecessary redirects that track users across the web.	6.1	More Details
CVE-2023-24086	SLIMS v9.5.2 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /customs/loan_by_class.php?reportView.	6.1	More Details
CVE-2023-23286	Cross Site Scripting (XSS) vulnerability in Provide server 14.4 allows attackers to execute arbitrary code through the server-log via username field from the login form.	6.1	More Details
CVE-2023-24648	Zstore v6.6.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /index.php.	6.1	More Details
CVE-2022-4286	A reflected cross-site scripting (XSS) vulnerability exists in System Diagnostics Manager of B&R Automation Runtime versions >=3.00 and <=C4.93 that enables a remote attacker to execute arbitrary JavaScript in the context of the users browser session.	6.1	More Details
CVE-2023-0099	The Simple URLs WordPress plugin before 115 does not sanitise and escape some parameters before outputting them back in some pages, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	6.1	More Details
CVE-2022-45087	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Group Arge Energy and Control Systems Smartpower Web allows Cross-Site Scripting (XSS). This issue affects Smartpower Web: before 23.01.01.	6.1	More Details
CVE-2022-45285	Vsourz Digital Advanced Contact form 7 DB Versions 1.7.2 and 1.9.1 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2023-24521	Due to insufficient input sanitization, SAP NetWeaver AS ABAP (BSP Framework) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an unauthenticated user to alter the current session of the user by injecting the malicious code over the network and gain access to the unintended data. This may lead to a limited impact on the confidentiality and the integrity of the application.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0624	OrangeScrum version 2.0.11 allows an external attacker to obtain arbitrary user accounts from the application. This is possible because the application returns malicious user input in the response with the content-type set to text/html.	6.1	More Details
CVE-2022-2094	The Yellow Yard Searchbar WordPress plugin before 2.8.2 does not escape some URL parameters before outputting them back to the user, leading to Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-34449	PowerPath Management Appliance with versions 3.3 & 3.2* contains a Hardcoded Cryptographic Keys vulnerability. Authenticated admin users can exploit the issue that leads to view and modifying sensitive information stored in the application.	6.0	More Details
CVE-2022-34445	Dell PowerScale OneFS, versions 8.2.x through 9.3.x contain a weak encoding for a password. A malicious local privileged attacker may potentially exploit this vulnerability, leading to information disclosure.	6.0	More Details
CVE-2023-0001	An information exposure vulnerability in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local system administrator to disclose the admin password for the agent in cleartext, which bad actors can then use to execute privileged cytool commands that disable or uninstall the agent.	6.0	More Details
CVE-2022-33216	Transient Denial-of-service in Automotive due to improper input validation while parsing ELF file.	6.0	More Details
CVE-2023-25563	GSS-NTLMSSP is a mechglue plugin for the GSSAPI library that implements NTLM authentication. Prior to version 1.2.0, multiple out-of-bounds reads when decoding NTLM fields can trigger a denial of service. A 32-bit integer overflow condition can lead to incorrect checks of consistency of length of internal buffers. Although most applications will error out before accepting a singe input buffer of 4GB in length this could theoretically happen. This vulnerability can be triggered via the main `gss_accept_sec_context` entry point if the application allows tokens greater than 4GB in length. This can lead to a large, up to 65KB, out-of-bounds read which could cause a denial-of-service if it reads from unmapped memory. Version 1.2.0 contains a patch for the out-of-bounds reads.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23625	go-unixfs is an implementation of a unix-like filesystem on top of an ipld merkledag. Trying to read malformed HAMT sharded directories can cause panics and virtual memory leaks. If you are reading untrusted user input, an attacker can then trigger a panic. This is caused by bogus `fanout` parameter in the HAMT directory nodes. Users are advised to upgrade to version 0.4.3 to resolve this issue. Users unable to upgrade should not feed untrusted user data to the decoding functions.	5.9	More Details
CVE-2023-23626	go-bitfield is a simple bitfield package for the go language aiming to be more performant that the standard library. When feeding untrusted user input into the size parameter of `NewBitfield` and `FromBytes` functions, an attacker can trigger `panic`s. This happen when the `size` is a not a multiple of `8` or is negative. There were already a note in the `NewBitfield` documentation, however known users of this package are subject to this issue. Users are advised to upgrade. Users unable to upgrade should ensure that `size` is a multiple of 8 before calling `NewBitfield` or `FromBytes`.	5.9	More Details
CVE-2023-23631	github.com/ipfs/go-unixfsnode is an ADL IPLD prime node that wraps go-codec-dagpb's implementation of protobuf to enable pathing. In versions priot to 1.5.2 trying to read malformed HAMT sharded directories can cause panics and virtual memory leaks. If you are reading untrusted user input, an attacker can then trigger a panic. This is caused by bogus fanout parameter in the HAMT directory nodes. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.9	More Details
CVE-2022-22564	Dell EMC Unity versions before 5.2.0.0.5.173 , use(es) broken cryptographic algorithm. A remote unauthenticated attacker could potentially exploit this vulnerability by performing MitM attacks and let attackers obtain sensitive information.	5.9	More Details
CVE-2023-22367	Ichiran App for iOS versions prior to 3.1.0 and Ichiran App for Android versions prior to 3.1.0 improperly verify server certificates, which may allow a remote unauthenticated attacker to eavesdrop on an encrypted communication via a man-in-the-middle attack.	5.9	More Details
CVE-2022-43552	A use after free vulnerability exists in curl <7.87.0. Curl can be asked to *tunnel* virtually all protocols it supports through an HTTP proxy. HTTP proxies can (and often do) deny such tunnel operations. When getting denied to tunnel the specific protocols SMB or TELNET, curl would use a heap-allocated struct after it had been freed, in its transfer shutdown code path.	5.9	More Details
CVE-2023-21421	Improper Handling of Insufficient Permissions or Privileges vulnerability in KnoxCustomManagerService prior to SMR Jan-2023 Release 1 allows attacker to access device SIM PIN.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23835	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.34), Mendix Applications using Mendix 8 (All versions < V8.18.23), Mendix Applications using Mendix 9 (All versions < V9.22.0), Mendix Applications using Mendix 9 (V9.12) (All versions < V9.12.10), Mendix Applications using Mendix 9 (V9.18) (All versions < V9.18.4), Mendix Applications using Mendix 9 (V9.6) (All versions < V9.6.15). Some of the Mendix runtime API's allow attackers to bypass XPath constraints and retrieve information using XPath queries that trigger errors.	5.9	More Details
CVE-2022-4304	A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.	5.9	More Details
CVE-2022-34444	Dell PowerScale OneFS, versions 9.2.0.x through 9.4.0.x contain an information vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability to cause data leak.	5.9	More Details
CVE-2023-25150	Nextcloud office/richdocuments is an office suit for the nextcloud server platform. In affected versions the Collabora integration can be tricked to provide access to any file without proper permission validation. As a result any user with access to Collabora can obtain the content of other users files. It is recommended that the Nextcloud Office App (Collabora Integration) is updated to 7.0.2 (Nextcloud 25), 6.3.2 (Nextcloud 24), 5.0.10 (Nextcloud 23), 4.2.9 (Nextcloud 21-22), or 3.8.7 (Nextcloud 15-20). There are no known workarounds for this issue.	5.8	More Details
CVE-2023-21693	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	5.7	More Details
CVE-2023-21422	Improper authorization vulnerability in semAddPublicDnsAddr in WifiSevice prior to SMR Jan-2023 Release 1 allows attackers to set custom DNS server without permission via binding WifiService.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25561	DataHub is an open-source metadata platform. In the event a system is using Java Authentication and Authorization Service (JAAS) authentication and that system is given a configuration which contains an error, the authentication for the system will fail open and allow an attacker to login using any username and password. The reason for this is that while an error is thrown in the `authenticateJaasUser` method it is swallowed without propagating the error. As a result of this issue unauthenticated users may gain access to the system. Users are advised to upgrade. There are no known workarounds for this issue. This vulnerability was discovered and reported by the GitHub Security lab and is tracked as GHSL-2022-081.	5.7	More Details
CVE-2023-21448	Path traversal vulnerability in Samsung Cloud prior to version 5.3.0.32 allows attacker to access specific png file.	5.7	More Details
CVE-2023-21567	Visual Studio Denial of Service Vulnerability	5.6	More Details
CVE-2022-47364	In wlan driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-44447	In wlan driver, there is a possible null pointer dereference issue due to a missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-44448	In wlan driver, there is a possible missing params check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-47357	In log service, there is a missing permission check. This could lead to local denial of service in log service.	5.5	More Details
CVE-2022-47359	In log service, there is a missing permission check. This could lead to local denial of service in log service.	5.5	More Details
CVE-2023-25166	formula is a math and string formula parser. In versions prior to 3.0.1 crafted user-provided strings to formula's parser might lead to polynomial execution time and a denial of service. Users should upgrade to 3.0.1+. There are no known workarounds for this vulnerability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47368	In wlan driver, there is a possible missing params check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-47356	In log service, there is a missing permission check. This could lead to local denial of service in log service.	5.5	More Details
CVE-2023-0818	Off-by-one Error in GitHub repository gpac/gpac prior to v2.3.0-DEV.	5.5	More Details
CVE-2022-47365	In wlan driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-42783	In wlan driver, there is a possible missing params check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-44421	In wlan driver, there is a possible missing permission check. This could lead to local In wlan driver, information disclosure.	5.5	More Details
CVE-2022-38675	In gpu driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-47369	In wlan driver, there is a possible missing params check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-47363	In wlan driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2015-10076	A vulnerability was found in dimtion Shaarlier up to 1.2.2. It has been declared as critical. Affected by this vulnerability is the function createTag of the file app/src/main/java/com/dimtion/shaarlier/TagsSource.java of the component Tag Handler. The manipulation leads to sql injection. Upgrading to version 1.2.3 is able to address this issue. The identifier of the patch is 3d1d9b239d9b3cd87e8bed45a0f02da583ad371e. It is recommended to upgrade the affected component. The identifier VDB-220453 was assigned to this vulnerability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47360	In log service, there is a missing permission check. This could lead to local denial of service in log service.	5.5	More Details
CVE-2022-47358	In log service, there is a missing permission check. This could lead to local denial of service in log service.	5.5	More Details
CVE-2022-47371	In bt driver, there is a thread competition leads to early release of resources to be accessed. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2023-23698	Dell Command | Update, Dell Update, and Alienware Update versions before 4.6.0 and 4.7.1 contain Insecure Operation on Windows Junction in the installer component. A local malicious user may potentially exploit this vulnerability leading to arbitrary file delete.	5.5	More Details
CVE-2022-38686	In wlan driver, there is a possible missing params check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-38681	In wlan driver, there is a possible missing params check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-38680	In wlan driver, there is a possible missing params check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-38674	In wlan driver, there is a possible missing params check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-47370	In wlan driver, there is a possible missing params check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-47323	In wlan driver, there is a possible missing params check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-47355	In log service, there is a missing permission check. This could lead to local denial of service in log service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47332	In wlan driver, there is a possible missing permission check. This could lead to local information disclosure.	5.5	More Details
CVE-2022-47346	In engineermode services, there is a missing permission check. This could lead to local denial of service in engineermode services.	5.5	More Details
CVE-2022-47451	In wlan driver, there is a possible missing params check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-47328	In wlan driver, there is a possible missing permission check. This could lead to local information disclosure.	5.5	More Details
CVE-2022-47329	In wlan driver, there is a possible missing permission check. This could lead to local information disclosure.	5.5	More Details
CVE-2022-47330	In wlan driver, there is a possible missing permission check. This could lead to local information disclosure.	5.5	More Details
CVE-2022-47452	In gnss driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-47333	In wlan driver, there is a possible missing permission check. This could lead to local information disclosure.	5.5	More Details
CVE-2022-47322	In wlan driver, there is a possible missing params check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-47342	In engineermode services, there is a missing permission check. This could lead to local denial of service in engineermode services.	5.5	More Details
CVE-2022-34392	SupportAssist for Home PCs (versions 3.11.4 and prior) contain an insufficient session expiration Vulnerability. An authenticated non-admin user can be able to obtain the refresh token and that leads to reuse the access token and fetch sensitive information.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47343	In engineermode services, there is a missing permission check. This could lead to local denial of service in engineermode services.	5.5	More Details
CVE-2023-21687	HTTP.sys Information Disclosure Vulnerability	5.5	More Details
CVE-2022-47344	In engineermode services, there is a missing permission check. This could lead to local denial of service in engineermode services.	5.5	More Details
CVE-2022-47345	In engineermode services, there is a missing permission check. This could lead to local denial of service in engineermode services.	5.5	More Details
CVE-2023-21445	Improper access control vulnerability in MyFiles prior to versions 12.2.09 in Android R(11), 13.1.03.501 in Android S(12) and 14.1.00.422 in Android T(13) allows local attacker to write file with MyFiles privilege via implicit intent.	5.5	More Details
CVE-2022-34386	Dell SupportAssist for Home PCs (version 3.11.4 and prior) and SupportAssist for Business PCs (version 3.2.0 and prior) contain cryptographic weakness vulnerability. An authenticated non-admin user could potentially exploit the issue and obtain sensitive information.	5.5	More Details
CVE-2022-47327	In wlan driver, there is a possible missing permission check. This could lead to local information disclosure.	5.5	More Details
CVE-2022-47325	In wlan driver, there is a possible missing permission check. This could lead to local information disclosure.	5.5	More Details
CVE-2022-34385	SupportAssist for Home PCs (version 3.11.4 and prior) and SupportAssist for Business PCs (version 3.2.0 and prior) contain cryptographic weakness vulnerability. An authenticated non-admin user could potentially exploit the issue and obtain sensitive information.	5.5	More Details
CVE-2022-47354	In log service, there is a missing permission check. This could lead to local denial of service in log service.	5.5	More Details
CVE-2022-47348	In engineermode services, there is a missing permission check. This could lead to local denial of service in engineermode services.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47367	In bluetooth driver, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-0002	A problem with a protection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local user to execute privileged cytool commands that disable or uninstall the agent.	5.5	More Details
CVE-2022-47324	In wlan driver, there is a possible missing permission check. This could lead to local information disclosure.	5.5	More Details
CVE-2023-21714	Microsoft Office Information Disclosure Vulnerability	5.5	More Details
CVE-2022-47450	In wlan driver, there is a possible missing permission check. This could lead to local information disclosure.	5.5	More Details
CVE-2022-47347	In engineermode services, there is a missing permission check. This could lead to local denial of service in engineermode services.	5.5	More Details
CVE-2023-24619	Redpanda before 22.3.12 discloses cleartext AWS credentials. The import functionality in the rpk binary logs an AWS Access Key ID and Secret in cleartext to standard output, allowing a local user to view the key in the console, or in Kubernetes logs if stdout output is collected. The fixed versions are 22.3.12, 22.2.10, and 22.1.12.	5.5	More Details
CVE-2022-47326	In wlan driver, there is a possible missing permission check. This could lead to local information disclosure.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22490	Git is a revision control system. Using a specially-crafted repository, Git prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8 can be tricked into using its local clone optimization even when using a non-local transport. Though Git will abort local clones whose source `$GIT_DIR/objects` directory contains symbolic links, the `objects` directory itself may still be a symbolic link. These two may be combined to include arbitrary files based on known paths on the victim's filesystem within the malicious repository's working copy, allowing for data exfiltration in a similar manner as CVE-2022-39253. A fix has been prepared and will appear in v2.39.2 v2.38.4 v2.37.6 v2.36.5 v2.35.7 v2.34.7 v2.33.7 v2.32.6, v2.31.7 and v2.30.8. If upgrading is impractical, two short-term workarounds are available. Avoid cloning repositories from untrusted sources with `--recurse-submodules`. Instead, consider cloning repositories without recursively cloning their submodules, and instead run `git submodule update` at each layer. Before doing so, inspect each new `.gitmodules` file to ensure that it does not contain suspicious module URLs.	5.5	More Details
CVE-2023-0747	Cross-site Scripting (XSS) - Stored in GitHub repository btcpayserver/btcpayserver prior to 1.7.6.	5.5	More Details
CVE-2022-47366	In wlan driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2023-0715	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_clone_folder function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the folder structure maintained by the plugin.	5.4	More Details
CVE-2023-21427	Improper access control vulnerability in NfcTile prior to SMR Jan-2023 Release 1 allows to attacker to use NFC without user recognition.	5.4	More Details
CVE-2023-0716	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_edit_folder function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the folder structure maintained by the plugin.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0726	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the ajax_edit_folder function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for administrators such as changing the folder structure maintained by the plugin.	5.4	More Details
CVE-2023-21571	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	5.4	More Details
CVE-2023-21570	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	5.4	More Details
CVE-2023-0725	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the ajax_clone_folder function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for administrators such as changing the folder structure maintained by the plugin.	5.4	More Details
CVE-2023-0724	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the ajax_add_folder function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for administrators such as changing the folder structure maintained by the plugin.	5.4	More Details
CVE-2023-0722	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the ajax_save_state function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for administrators such as changing the folder structure maintained by the plugin.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22942	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, a cross-site request forgery in the Splunk Secure Gateway (SSG) app in the 'kvstore_client' REST endpoint lets a potential attacker update SSG KV store collections using an HTTP GET request.	5.4	More Details
CVE-2022-41620	Cross-Site Request Forgery (CSRF) vulnerability in SeoSamba for WordPress Webmasters plugin <= 1.0.5 versions.	5.4	More Details
CVE-2023-0717	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_delete_folder function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the folder structure maintained by the plugin.	5.4	More Details
CVE-2023-24687	Mojoportal v2.7.0.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Company Info Settings component. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the txtCompanyName parameter.	5.4	More Details
CVE-2023-0827	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 1.5.17.	5.4	More Details
CVE-2023-25065	Cross-Site Request Forgery (CSRF) vulnerability in ShapedPlugin WP Tabs – Responsive Tabs Plugin for WordPress plugin <= 2.1.14 versions.	5.4	More Details
CVE-2023-21573	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	5.4	More Details
CVE-2023-24690	ChurchCRM 4.5.3 and below was discovered to contain a stored cross-site scripting (XSS) vulnerability at /api/public/register/family.	5.4	More Details
CVE-2023-0720	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_save_folder_order function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the folder structure maintained by the plugin.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24382	Cross-Site Request Forgery (CSRF) vulnerability in Photon WP Material Design Icons for Page Builders plugin <= 1.4.2 versions.	5.4	More Details
CVE-2022-45755	Cross-site scripting (XSS) vulnerability in EyouCMS v1.6.0 allows attackers to execute arbitrary code via the home page description on the basic information page.	5.4	More Details
CVE-2023-0360	The Location Weather WordPress plugin before 1.3.4 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2022-4562	The Meks Flexible Shortcodes WordPress plugin before 1.3.5 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2023-0169	The Zoho Forms WordPress plugin before 3.0.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2022-4656	The WP Visitor Statistics (Real Time Traffic) WordPress plugin before 6.5 does not validate and escape one of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attack.	5.4	More Details
CVE-2022-45086	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Group Arge Energy and Control Systems Smartpower Web allows Cross-Site Scripting (XSS). This issue affects Smartpower Web: before 23.01.01.	5.4	More Details
CVE-2022-4678	The TemplatesNext ToolKit WordPress plugin before 3.2.8 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2022-4682	The Lightbox Gallery WordPress plugin before 0.9.5 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45091	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Group Arge Energy and Control Systems Smartpower Web allows Cross-Site Scripting (XSS).This issue affects Smartpower Web: before 23.01.01.	5.4	More Details
CVE-2023-0685	The Wicked Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.18.16. This is due to missing or incorrect nonce validation on the ajax_unassign_folders function. This makes it possible for unauthenticated attackers to invoke this function via forged request granted they can trick a site administrator into performing an action such as clicking on a link leading them to perform actions intended for administrators such as changing the folder structure maintained by the plugin..	5.4	More Details
CVE-2023-25572	react-admin is a frontend framework for building browser applications on top of REST/GraphQL APIs. react-admin prior to versions 3.19.12 and 4.7.6, along with ra-ui-materialui prior to 3.19.12 and 4.7.6, are vulnerable to cross-site scripting. All React applications built with react-admin and using the `<RichTextField>` are affected. `<RichTextField>` outputs the field value using `dangerouslySetInnerHTML` without client-side sanitization. If the data isn't sanitized server-side, this opens a possible cross-site scripting (XSS) attack. Versions 3.19.12 and 4.7.6 now use `DOMPurify` to escape the HTML before outputting it with React and `dangerouslySetInnerHTML`. Users who already sanitize HTML data server-side do not need to upgrade. As a workaround, users may replace the `<RichTextField>` by a custom field doing sanitization by hand.	5.4	More Details
CVE-2022-4759	The GigPress WordPress plugin before 2.3.28 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-0684	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_unassign_folders function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as changing the folder structure maintained by the plugin.	5.4	More Details
CVE-2022-4783	The Youtube Channel Gallery WordPress plugin through 2.4 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0718	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_save_folder function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the folder structure maintained by the plugin.	5.4	More Details
CVE-2023-0810	Cross-site Scripting (XSS) - Stored in GitHub repository btcpayserver/btcpayserver prior to 1.7.11.	5.4	More Details
CVE-2022-41134	Cross-Site Request Forgery (CSRF) in OptinlyHQ Optinly – Exit Intent, Newsletter Popups, Gamification & Opt-in Forms plugin <= 1.0.15 versions.	5.4	More Details
CVE-2022-4830	The Paid Memberships Pro WordPress plugin before 2.9.9 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2023-0379	The Spotlight Social Feeds WordPress plugin before 1.4.3 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-0373	The Lightweight Accordion WordPress plugin before 1.5.15 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-0034	The JetWidgets For Elementor WordPress plugin before 1.0.14 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-0060	The Responsive Gallery Grid WordPress plugin before 2.3.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0362	Themify Portfolio Post WordPress plugin before 1.2.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-0061	The Judge.me Product Reviews for WooCommerce WordPress plugin before 1.3.21 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-0333	The TemplatesNext ToolKit WordPress plugin before 3.2.9 does not validate some of its shortcode attributes before using them to generate an HTML tag, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-0075	The Amazon JS WordPress plugin through 0.10 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-0275	The Easy Accept Payments for PayPal WordPress plugin before 4.9.10 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-0270	The YaMaps for WordPress Plugin WordPress plugin before 0.6.26 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-0151	The uTubeVideo Gallery WordPress plugin before 2.0.8 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-0166	The Product Slider for WooCommerce by PickPlugins WordPress plugin before 1.13.42 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4580	The Twenty20 Image Before-After WordPress plugin through 1.5.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-4628	The Easy PayPal Buy Now Button WordPress plugin before 1.7.4 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-0177	The Social Like Box and Page by WpDevArt WordPress plugin before 0.8.41 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2022-4512	The Better Font Awesome WordPress plugin before 2.0.4 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-0711	The Wicked Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the ajax_save_state function in versions up to, and including, 2.18.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke this function and perform actions intended for administrators such as modifying the view state of the folder structure maintained by the plugin.	5.4	More Details
CVE-2022-4448	The GiveWP WordPress plugin before 2.24.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-4458	The amr shortcode any widget WordPress plugin through 4.0 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43469	Cross-Site Request Forgery (CSRF) vulnerability in Orchestrated Corona Virus (COVID-19) Banner & Live Data plugin <= 1.7.0.6 versions.	5.4	More Details
CVE-2023-0780	Improper Restriction of Rendered UI Layers or Frames in GitHub repository cockpit-hq/cockpit prior to 2.3.9-dev.	5.4	More Details
CVE-2022-4471	The YARPP WordPress plugin before 5.30.3 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-25727	In phpMyAdmin before 4.9.11 and 5.x before 5.2.1, an authenticated user can trigger XSS by uploading a crafted .sql file through the drag-and-drop interface.	5.4	More Details
CVE-2022-4473	The Widget Shortcode WordPress plugin through 0.3.5 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4488	The Widgets on Pages WordPress plugin before 1.8.0 does not validate and escape its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-45724	Incorrect Access Control in Comfast router CF-WR6110N V2.3.1 allows a remote attacker on the same network to perform any HTTP request to an unauthenticated page to force the server to generate a SESSION_ID, and using this SESSION_ID an attacker can then perform authenticated requests.	5.4	More Details
CVE-2022-4551	The Rich Table of Contents WordPress plugin before 1.3.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23851	SAP Business Planning and Consolidation - versions 200, 300, allows an attacker with business authorization to upload any files (including web pages) without the proper file format validation. If other users visit the uploaded malicious web page, the attacker may perform actions on behalf of the users without their consent impacting the confidentiality and integrity of the system.	5.4	More Details
CVE-2023-0655	SonicWall Email Security contains a vulnerability that could permit a remote unauthenticated attacker access to an error page that includes sensitive information about users email addresses.	5.3	More Details
CVE-2022-3891	The WP FullCalendar WordPress plugin before 1.5 does not ensure that the post retrieved via an AJAX action is public and can be accessed by the user making the request, allowing unauthenticated attackers to get the content of arbitrary posts, including draft/private as well as password-protected ones.	5.3	More Details
CVE-2018-7935	There is a vulnerability in 21.328.01.00.00 version of the E5573Cs-322. Remote attackers could exploit this vulnerability to make the network where the E5573Cs-322 is running temporarily unavailable.	5.3	More Details
CVE-2022-46675	Wyse Management Suite Repository 3.8 and below contain an information disclosure vulnerability. A unauthenticated attacker could potentially discover the internal structure of the application and its components and use this information for further vulnerability research.	5.3	More Details
CVE-2022-34350	IBM API Connect 10.0.0.0 through 10.0.5.0, 10.0.1.0 through 10.0.1.7, and 2018.4.1.0 through 2018.4.1.20 is vulnerable to External Service Interaction attack, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to induce the application to perform server-side DNS lookups or HTTP requests to arbitrary domain names. By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with. IBM X-Force ID: 230264.	5.3	More Details
CVE-2022-45190	An issue was discovered on Microchip RN4870 1.43 devices. An attacker within BLE radio range can bypass passkey entry in the legacy pairing of the device.	5.3	More Details
CVE-2022-48296	The SystemUI has a vulnerability in permission management. Successful exploitation of this vulnerability may cause users to receive broadcasts from malicious apps, conveying false alarm information about external storage devices.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21720	Microsoft Edge (Chromium-based) Tampering Vulnerability	5.3	More Details
CVE-2022-30564	Some Dahua embedded products have a vulnerability of unauthorized modification of the device timestamp. By sending a specially crafted packet to the vulnerable interface, an attacker can modify the device system time.	5.3	More Details
CVE-2023-24688	An issue in Mojoportal v2.7.0.0 allows an unauthenticated attacker to register a new user even if the Allow User Registrations feature is disabled.	5.3	More Details
CVE-2023-25162	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. Nextcloud Server prior to 24.0.8 and 23.0.12 and Nextcloud Enterprise server prior to 24.0.8 and 23.0.12 are vulnerable to server-side request forgery (SSRF). Attackers can leverage enclosed alphanumeric payloads to bypass IP filters and gain SSRF, which would allow an attacker to read crucial metadata if the server is hosted on the AWS platform. Nextcloud Server 24.0.8 and 23.0.2 and Nextcloud Enterprise Server 24.0.8 and 23.0.12 contain a patch for this issue. No known workarounds are available.	5.3	More Details
CVE-2023-21699	Windows Internet Storage Name Service (iSNS) Server Information Disclosure Vulnerability	5.3	More Details
CVE-2023-22370	Stored cross-site scripting vulnerability in Wired/Wireless LAN Pan/Tilt Network Camera CS-WMV02G all versions allows a network-adjacent authenticated attacker to inject an arbitrary script. NOTE: This vulnerability only affects products that are no longer supported by the developer.	5.2	More Details
CVE-2023-21423	Improper authorization vulnerability in ChnFileShareKit prior to SMR Jan-2023 Release 1 allows attacker to control BLE advertising without permission using unprotected action.	5.1	More Details
CVE-2023-21424	Improper Handling of Insufficient Permissions or Privileges vulnerability in SemChameleonHelper prior to SMR Jan-2023 Release 1 allows attacker to modify network related values, network code, carrier id and operator brand.	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0690	HashiCorp Boundary from 0.10.0 through 0.11.2 contain an issue where when using a PKI-based worker with a Key Management Service (KMS) defined in the configuration file, new credentials created after an automatic rotation may not have been encrypted via the intended KMS. This would result in the credentials being stored in plaintext on the Boundary PKI worker's disk. This issue is fixed in version 0.12.0.	5.0	More Details
CVE-2022-42292	NVIDIA GeForce Experience contains a vulnerability in the NVContainer component, where a user without administrator privileges can create a symbolic link to a file that requires elevated privileges to write to or modify, which may lead to denial of service, escalation of privilege or limited data tampering.	5.0	More Details
CVE-2023-21722	.NET Framework Denial of Service Vulnerability	5.0	More Details
CVE-2022-4903	A vulnerability was found in CodenameOne 7.0.70. It has been classified as problematic. Affected is an unknown function. The manipulation leads to use of implicit intent for sensitive communication. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. Upgrading to version 7.0.71 is able to address this issue. The patch is identified as dad49c9ef26a598619fc48d2697151a02987d478. It is recommended to upgrade the affected component. VDB-220470 is the identifier assigned to this vulnerability.	5.0	More Details
CVE-2023-24804	The ownCloud Android app allows ownCloud users to access, share, and edit files and folders. Prior to version 3.0, the app has an incomplete fix for a path traversal issue and is vulnerable to two bypass methods. The bypasses may lead to information disclosure when uploading the app's internal files, and to arbitrary file write when uploading plain text files (although limited by the .txt extension). Version 3.0 fixes the reported bypasses.	5.0	More Details
CVE-2022-46755	Wyse Management Suite 3.8 and below contain an improper access control vulnerability. A authenticated malicious admin user can edit general client policy for which the user is not authorized.	4.9	More Details
CVE-2022-46678	Wyse Management Suite 3.8 and below contain an improper access control vulnerability. A authenticated malicious admin user can edit general client policy for which the user is not authorized.	4.9	More Details
CVE-2022-46650	Acemanager in ALEOS before version 4.16 allows a user with valid credentials to reconfigure the device to expose the ACEManager credentials on the pre-login status page.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42444	IBM App Connect Enterprise 11.0.0.8 through 11.0.0.19 and 12.0.1.0 through 12.0.5.0 is vulnerable to a buffer overflow. A remote privileged user could overflow a buffer and cause the application to crash. IBM X-Force ID: 238538.	4.9	More Details
CVE-2022-46676	Wyse Management Suite 3.8 and below contain an improper access control vulnerability. A malicious admin user can disable or delete users under administration and unassigned admins for which the group admin is not authorized.	4.9	More Details
CVE-2023-24815	Vert.x-Web is a set of building blocks for building web applications in the java programming language. When running vertx web applications that serve files using `StaticHandler` on Windows Operating Systems and Windows File Systems, if the mount point is a wildcard (`*`) then an attacker can exfiltrate any class path resource. When computing the relative path to locate the resource, in case of wildcards, the code: `return "/" + rest;` from `Utils.java` returns the user input (without validation) as the segment to lookup. Even though checks are performed to avoid escaping the sandbox, given that the input was not sanitized `\` are not properly handled and an attacker can build a path that is valid within the classpath. This issue only affects users deploying in windows environments and upgrading is the advised remediation path. There are no known workarounds for this vulnerability.	4.8	More Details
CVE-2022-34451	PowerPath Management Appliance with versions 3.3 & 3.2*, 3.1 & 3.0* contains a Stored Cross-site Scripting Vulnerability. An authenticated admin user could potentially exploit this vulnerability, to hijack user sessions or trick a victim application user into unknowingly send arbitrary requests to the server.	4.8	More Details
CVE-2023-24232	A stored cross-site scripting (XSS) vulnerability in the component /php-inventory-management-system/product.php of Inventory Management System v1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Product Name parameter.	4.8	More Details
CVE-2023-24234	A stored cross-site scripting (XSS) vulnerability in the component php-inventory-management-system/brand.php of Inventory Management System v1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Brand Name parameter.	4.8	More Details
CVE-2023-24233	A stored cross-site scripting (XSS) vulnerability in the component /php-inventory-management-system/orders.php?o=add of Inventory Management System v1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Client Name parameter.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24686	An issue in the CSV Import function of ChurchCRM v4.5.3 and below allows attackers to execute arbitrary code via importing a crafted CSV file.	4.8	More Details
CVE-2023-22943	In Splunk Add-on Builder (AoB) versions below 4.1.2 and the Splunk CloudConnect SDK versions below 3.1.3, requests to third-party APIs through the REST API Modular Input incorrectly revert to using HTTP to connect after a failure to connect over HTTPS occurs.	4.8	More Details
CVE-2023-24230	A stored cross-site scripting (XSS) vulnerability in the component /formwork/panel/dashboard of Formwork v1.12.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Page title parameter.	4.8	More Details
CVE-2023-24231	A stored cross-site scripting (XSS) vulnerability in the component /php-inventory-management-system/categories.php of Inventory Management System v1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Categories Name parameter.	4.8	More Details
CVE-2023-23697	Dell Command | Intel vPro Out of Band, versions before 4.4.0, contain an arbitrary folder delete vulnerability during uninstallation. A locally authenticated malicious user may potentially exploit this vulnerability leading to arbitrary folder deletion.	4.7	More Details
CVE-2023-24572	Dell Command | Integration Suite for System Center, versions before 6.4.0 contain an arbitrary folder delete vulnerability during uninstallation. A locally authenticated malicious user may potentially exploit this vulnerability leading to arbitrary folder deletion.	4.7	More Details
CVE-2023-0783	A vulnerability was found in EcShop 4.1.5. It has been classified as critical. This affects an unknown part of the file /ecshop/admin/template.php of the component PHP File Handler. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-220641 was assigned to this vulnerability.	4.7	More Details
CVE-2022-47331	In wlan driver, there is a race condition. This could lead to local denial of service in wlan services.	4.7	More Details
CVE-2023-24573	Dell Command | Monitor versions prior to 10.9 contain an arbitrary folder delete vulnerability during uninstallation. A locally authenticated malicious user may potentially exploit this vulnerability leading to arbitrary folder deletion.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34362	IBM Sterling Secure Proxy 6.0.3 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 230523.	4.6	More Details
CVE-2023-23475	IBM Infosphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 245423.	4.6	More Details
CVE-2023-24816	IPython (Interactive Python) is a command shell for interactive computing in multiple programming languages, originally developed for the Python programming language. Versions prior to 8.1.0 are subject to a command injection vulnerability with very specific prerequisites. This vulnerability requires that the function `IPython.utils.terminal.set_term_title` be called on Windows in a Python environment where ctypes is not available. The dependency on `ctypes` in `IPython.utils._process_win32` prevents the vulnerable code from ever being reached in the ipython binary. However, as a library that could be used by another tool `set_term_title` could be called and hence introduce a vulnerability. Should an attacker get untrusted input to an instance of this function they would be able to inject shell commands as current process and limited to the scope of the current process. Users of ipython as a library are advised to upgrade. Users unable to upgrade should ensure that any calls to the `IPython.utils.terminal.set_term_title` function are done with trusted or filtered input.	4.5	More Details
CVE-2023-23553	Control By Web X-400 devices are vulnerable to a cross-site scripting attack, which could result in private and session information being transferred to the attacker.	4.5	More Details
CVE-2022-34364	Dell BSAFE SSL-J, versions before 6.5 and version 7.0 contain a debug message revealing unnecessary information vulnerability. This may lead to disclosing sensitive information to a locally privileged user. .	4.4	More Details
CVE-2023-21435	Exposure of Sensitive Information vulnerability in Fingerprint TA prior to SMR Feb-2023 Release 1 allows attackers to access the memory address information via log.	4.4	More Details
CVE-2023-21430	An out-of-bound read vulnerability in mapToBuffer function in libSDKRecognitionText.spensdk.samsung.so library prior to SMR JAN-2023 Release 1 allows attacker to cause memory access fault.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23856	In SAP BusinessObjects Business Intelligence (Web Intelligence user interface) - version 430, some calls return json with wrong content type in the header of the response. As a result, a custom application that calls directly the jsp of Web Intelligence DHTML may be vulnerable to XSS attacks. On successful exploitation an attacker can cause a low impact on integrity of the application.	4.3	More Details
CVE-2023-21794	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4.3	More Details
CVE-2023-25165	Helm is a tool that streamlines installing and managing Kubernetes applications.`getHostByName` is a Helm template function introduced in Helm v3. The function is able to accept a hostname and return an IP address for that hostname. To get the IP address the function performs a DNS lookup. The DNS lookup happens when used with `helm installlupgradeltemplate` or when the Helm SDK is used to render a chart. Information passed into the chart can be disclosed to the DNS servers used to lookup the IP address. For example, a malicious chart could inject `getHostByName` into a chart in order to disclose values to a malicious DNS server. The issue has been fixed in Helm 3.11.1. Prior to using a chart with Helm verify the `getHostByName` function is not being used in a template to disclose any information you do not want passed to DNS servers.	4.3	More Details
CVE-2019-25103	A vulnerability has been found in simple-markdown 0.5.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file simple-markdown.js. The manipulation leads to inefficient regular expression complexity. The attack can be launched remotely. Upgrading to version 0.5.2 is able to address this issue. The patch is named 89797fef9abb4cab2fb76a335968266a92588816. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-220639.	4.3	More Details
CVE-2023-25066	Cross-Site Request Forgery (CSRF) vulnerability in FolioVision FV Flowplayer Video Player plugin <= 7.5.30.7212 versions.	4.3	More Details
CVE-2023-24525	SAP CRM WebClient UI - versions WEBCUIF 748, 800, 801, S4FND 102, 103, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an authenticated attacker can cause limited impact on confidentiality of the application.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-25102	A vulnerability, which was classified as problematic, was found in simple-markdown 0.6.0. Affected is an unknown function of the file simple-markdown.js. The manipulation with the input <<<<<<<<<<:/:/:/:/:/:/:/:/:/ leads to inefficient regular expression complexity. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 0.6.1 is able to address this issue. The patch is identified as 015a719bf5cdc561feea05500ecb3274ef609cd2. It is recommended to upgrade the affected component. VDB-220638 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2023-22938	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the ‘sendemail’ REST API endpoint lets any authenticated user send an email as the Splunk instance. The endpoint is now restricted to the ‘splunk-system-user’ account on the local instance.	4.3	More Details
CVE-2023-0518	An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.0 before 15.6.7, all versions starting from 15.7 before 15.7.6, all versions starting from 15.8 before 15.8.1. It was possible to trigger a DoS attack by uploading a malicious Helm chart.	4.3	More Details
CVE-2022-3759	An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.3 before 15.6.7, all versions starting from 15.7 before 15.7.6, all versions starting from 15.8 before 15.8.1. An attacker may upload a crafted CI job artifact zip file in a project that uses dynamic child pipelines and make a sidekiq job allocate a lot of memory. In GitLab instances where Sidekiq is memory-limited, this may cause Denial of Service.	4.3	More Details
CVE-2023-24689	An issue in Mojoportal v2.7.0.0 and below allows an authenticated attacker to list all css files inside the root path of the webserver via manipulation of the "s" parameter in /DesignTools/ManageSkin.aspx	4.3	More Details
CVE-2022-46862	Cross-Site Request Forgery (CSRF) vulnerability in ExpressTech Quiz And Survey Master – Best Quiz, Exam and Survey Plugin for WordPress plugin <= 8.0.7 versions.	4.3	More Details
CVE-2023-21419	An improper implementation logic in Secure Folder prior to SMR Jan-2023 Release 1 allows the Secure Folder container remain unlocked under certain condition.	4.3	More Details
CVE-2023-24377	Cross-Site Request Forgery (CSRF) vulnerability in Ecwid Ecommerce Ecwid Ecommerce Shopping Cart plugin <= 6.11.3 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21426	Hardcoded AES key to encrypt cardemulation PINs in NFC prior to SMR Jan-2023 Release 1 allows attackers to access cardemulation PIN.	4.3	More Details
CVE-2023-22937	In Splunk Enterprise versions below 8.1.13, 8.2.10, and 9.0.4, the lookup table upload feature let a user upload lookup tables with unnecessary filename extensions. Lookup table file extensions may now be one of the following only: .csv, .csv.gz, .kmz, .kml, .mmdb, or .mmdb.gzl.	4.3	More Details
CVE-2023-21425	Improper access control vulnerability in telecom application prior to SMR JAN-2023 Release 1 allows local attackers to get sensitive information.	4.3	More Details
CVE-2023-22931	In Splunk Enterprise versions below 8.1.13 and 8.2.10, the ‘createrss’ external search command overwrites existing Resource Description Format Site Summary (RSS) feeds without verifying permissions. This feature has been deprecated and disabled by default.	4.3	More Details
CVE-2023-0405	The GPT AI Power: Content Writer & ChatGPT & Image Generator & WooCommerce Product Writer & AI Training WordPress plugin before 1.4.38 does not perform any kind of nonce or privilege checks before letting logged-in users modify arbitrary posts.	4.3	More Details
CVE-2023-21432	Improper access control vulnerabilities in Smart Things prior to 1.7.93 allows to attacker to invite others without authorization of the owner.	4.2	More Details
CVE-2023-25758	Onekey Touch devices through 4.0.0 and Onekey Mini devices through 2.10.0 allow man-in-the-middle attackers to obtain the seed phase. The man-in-the-middle access can only be obtained after disassembling a device (i.e., here, "man-in-the-middle" does not refer to the attacker's position on an IP network). NOTE: the vendor states that "our hardware team has updated the security patch without anyone being affected."	4.2	More Details
CVE-2023-25160	Nextcloud Mail is an email app for the Nextcloud home server platform. Prior to versions 2.2.1, 1.14.5, 1.12.9, and 1.11.8, an attacker can access the mail box by ID getting the subjects and the first characters of the emails. Users should upgrade to Mail 2.2.1 for Nextcloud 25, Mail 1.14.5 for Nextcloud 22-24, Mail 1.12.9 for Nextcloud 21, or Mail 1.11.8 for Nextcloud 20 to receive a patch. No known workarounds are available.	4.1	More Details
CVE-2023-21429	Improper usage of implict intent in ePDG prior to SMR JAN-2023 Release 1 allows attacker to access SSID.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21428	Improper input validation vulnerability in TelephonyUI prior to SMR Jan-2023 Release 1 allows attackers to configure Preferred Call. The patch removes unused code.	4.0	More Details
CVE-2023-21442	Improper access control vulnerability in Runestone application prior to version 2.9.09.003 in Android R(11) and 3.2.01.007 in Android S(12) allows local attackers to get device location information.	4.0	More Details
CVE-2023-21437	Improper access control vulnerability in Phone application prior to SMR Feb-2023 Release 1 allows local attackers to access sensitive information via implicit broadcast.	4.0	More Details
CVE-2023-21447	Improper access control vulnerabilities in Samsung Cloud prior to version 5.3.0.32 allows local attackers to access information with Samsung Cloud's privilege via implicit intent.	4.0	More Details
CVE-2022-42436	IBM MQ 8.0.0, 9.0.0, 9.1.0, 9.2.0, 9.3.0 Managed File Transfer could allow a local user to obtain sensitive information from diagnostic files. IBM X-Force ID: 238206.	4.0	More Details
CVE-2023-0808	A vulnerability was found in Deye/Revolt/Bosswerk Inverter MW3_15U_5406_1.47/MW3_15U_5406_1.471. It has been rated as problematic. This issue affects some unknown processing of the component Access Point Setting Handler. The manipulation with the input 12345678 leads to use of hard-coded password. It is possible to launch the attack on the physical device. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. Upgrading to version MW3_16U_5406_1.53 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-220769 was assigned to this vulnerability.	3.9	More Details
CVE-2022-34376	Dell PowerEdge BIOS and Dell Precision BIOS contain an improper input validation vulnerability. A local authenticated malicious user may potentially exploit this vulnerability by manipulating an SMI to cause a denial of service during SMM.	3.9	More Details
CVE-2023-23854	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	3.8	More Details
CVE-2022-34389	Dell SupportAssist contains a rate limit bypass issues in screenmeet API third party component. An unauthenticated attacker could potentially exploit this vulnerability and impersonate a legitimate dell customer to a dell support technician.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0785	A vulnerability classified as problematic was found in SourceCodester Best Online News Portal 1.0. Affected by this vulnerability is an unknown functionality of the file check_availability.php. The manipulation of the argument username leads to exposure of sensitive information through data queries. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-220645 was assigned to this vulnerability.	3.7	More Details
CVE-2023-25161	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform. Nextcloud Server and Nextcloud Enterprise Server prior to versions 25.0.1 24.0.8, and 23.0.12 missing rate limiting on password reset functionality. This could result in service slowdown, storage overflow, or cost impact when using external email services. Users should upgrade to Nextcloud Server 25.0.1, 24.0.8, or 23.0.12 or Nextcloud Enterprise Server 25.0.1, 24.0.8, or 23.0.12 to receive a patch. No known workarounds are available.	3.7	More Details
CVE-2015-10078	A vulnerability, which was classified as problematic, has been found in atwellpub Resend Welcome Email Plugin 1.0.1 on WordPress. This issue affects the function send_welcome_email_url of the file resend-welcome-email.php. The manipulation leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 1.0.2 is able to address this issue. The identifier of the patch is b14c1f66d307783f0ae74f88088a85999107695c. It is recommended to upgrade the affected component. The identifier VDB-220637 was assigned to this vulnerability.	3.5	More Details
CVE-2020-36661	A vulnerability was found in Kong lua-multipart 0.5.8-1. It has been declared as problematic. This vulnerability affects the function is_header of the file src/multipart.lua. The manipulation leads to inefficient regular expression complexity. Upgrading to version 0.5.9-1 is able to address this issue. The patch is identified as d632e5df43a2928fd537784a99a79dec288bf01b. It is recommended to upgrade the affected component. VDB-220642 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4905	A vulnerability was found in UDX Stateless Media Plugin 3.1.1 on WordPress. It has been declared as problematic. This vulnerability affects the function setup_wizard_interface of the file lib/classes/class-settings.php. The manipulation of the argument settings leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 3.2.0 is able to address this issue. The patch is identified as 6aee7ae0b0beeb2232ce6e1c82aa7e2041ae151a. It is recommended to upgrade the affected component. VDB-220750 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2015-10079	A vulnerability was found in juju2143 WalrusIRC 0.0.2. It has been rated as problematic. This issue affects the function parseLinks of the file public/parser.js. The manipulation of the argument text leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 0.0.3 is able to address this issue. The patch is named 45fd885895ae13e8d9b3a71e89d59768914f60af. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-220751.	3.5	More Details
CVE-2023-21436	Improper usage of implicit intent in Contacts prior to SMR Feb-2023 Release 1 allows attacker to get account ID.	3.3	More Details
CVE-2023-24565	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2022 (All versions), Solid Edge SE2023 (All versions < V223.0Update2). The affected application contains an out of bounds read past the end of an allocated buffer while parsing a specially crafted STL file. This vulnerability could allow an attacker to disclose sensitive information. (ZDI-CAN-19428)	3.3	More Details
CVE-2023-24566	A vulnerability has been identified in Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2022 (All versions), Solid Edge SE2023 (All versions < V223.0Update2). The affected application is vulnerable to stack-based buffer while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19472)	3.3	More Details
CVE-2023-21431	Improper input validation in Bixby Vision prior to version 3.7.70.17 allows attacker to access data of Bixby Vision.	3.3	More Details
CVE-2022-34452	PowerPath Management Appliance with versions 3.3, 3.2*, 3.1 & 3.0* contains sensitive information disclosure vulnerability. An Authenticated admin user can able to exploit the issue and view sensitive information stored in the logs.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23934	Werkzeug is a comprehensive WSGI web application library. Browsers may allow "nameless" cookies that look like `=value` instead of `key=value`. A vulnerable browser may allow a compromised application on an adjacent subdomain to exploit this to set a cookie like `=__Host-test=bad` for another subdomain. Werkzeug prior to 2.2.3 will parse the cookie `=__Host-test=bad` as __Host-test=bad`. If a Werkzeug application is running next to a vulnerable or malicious subdomain which sets such a cookie using a vulnerable browser, the Werkzeug application will see the bad cookie value but the valid cookie key. The issue is fixed in Werkzeug 2.2.3.	2.6	More Details
CVE-2022-35720	IBM Sterling External Authentication Server 6.1.0 and IBM Sterling Secure Proxy 6.0.3 uses weaker than expected cryptographic algorithms during installation that could allow a local attacker to decrypt sensitive information. IBM X-Force ID: 231373.	2.3	More Details
CVE-2023-25159	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Office is a document collaboration app for the same platform. Nextcloud Server 24.0.x prior to 24.0.8 and 25.0.x prior to 25.0.1, Nextcloud Enterprise Server 24.0.x prior to 24.0.8 and 25.0.x prior to 25.0.1, and Nextcloud Office (Richdocuments) App 6.x prior to 6.3.1 and 7.x prior to 7.0.1 have previews accessible without a watermark. The download should be hidden and the watermark should get applied. This issue is fixed in Nextcloud Server 25.0.1 and 24.0.8, Nextcloud Enterprise Server 25.0.1 and 24.0.8, and Nextcloud Office (Richdocuments) App 7.0.1 (for 25) and 6.3.1 (for 24). No known workarounds are available.	2.3	More Details
CVE-2023-21450	Missing Authorization vulnerability in One Hand Operation + prior to version 6.1.21 allows multi-users to access owner's widget without authorization via gesture setting.	2.3	More Details
CVE-2023-21438	Improper logic in HomeScreen prior to SMR Feb-2023 Release 1 allows physical attacker to access App preview protected by Secure Folder.	2.1	More Details
CVE-2022-34377	Dell PowerEdge BIOS and Dell Precision BIOS contain an Improper SMM communication buffer verification vulnerability. A local malicious user with high Privileges may potentially exploit this vulnerability to perform arbitrary code execution or cause denial of service.	1.9	More Details
CVE-2023-22609	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 Number	Description	Base Score	Reference
CVE-2021-41064	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2023-22369	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-25011. Reason: This candidate is a duplicate of CVE-2023-25011. Notes: All CVE users should reference CVE-2023-25011 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-22607	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-2023-22606	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-2023-22605	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-2022-4133	Rejected reason: We were unable to verify this vulnerbility.	N/A	More Details
CVE-2023-22604	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-2023-22603	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2021-42793	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2023-0680	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-42792	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25723	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-2023-25724	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