SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 15 March 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-2023-1283	Code Injection in GitHub repository builderio/qwik prior to 0.21.0.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27482	homeassistant is an open source home automation tool. A remotely exploitable vulnerability bypassing authentication for accessing the Supervisor API through Home Assistant has been discovered. This impacts all Home Assistant installation types that use the Supervisor 2023.01.1 or older. Installation types, like Home Assistant Container (for example Docker), or Home Assistant Core manually in a Python environment, are not affected. The issue has been mitigated and closed in Supervisor version 2023.03.1, which has been rolled out to all affected installations via the auto-update feature of the Supervisor. This rollout has been completed at the time of publication of this advisory. Home Assistant Core 2023.3.0 included mitigation for this vulnerability. Upgrading to at least that version is thus advised. In case one is not able to upgrade the Home Assistant Supervisor or the Home Assistant Core application at this time, it is advised to not expose your Home Assistant instance to the internet.	10.0	More Details
CVE-2023-	wasmtime is a fast and secure runtime for WebAssembly. In affected versions wasmtime's code generator, Cranelift, has a bug on x86_64 targets where address-mode computation mistakenly would calculate a 35-bit effective address instead of WebAssembly's defined 33-bit effective address. This bug means that, with default codegen settings, a wasm-controlled load/store operation could read/write addresses up to 35 bits away from the base of linear memory. Due to this bug, however, addresses up to `0xffffffff * 8 + 0x7ffffffc = 36507222004 = ~34G` bytes away from the base of linear memory are possible from guest code. This means that the virtual memory 6G away from the base of linear memory up to ~34G away can be read/written by a malicious module. A guest module can, without the knowledge of the embedder, read/write memory in this region. The memory may belong to other WebAssembly instances when using the pooling allocator, for example. Affected embedders are recommended to analyze preexisting wasm modules to see if they're affected by the incorrect codegen rules and possibly correlate that with an anomalous number of traps during historical execution to locate possibly suspicious modules. The specific bug in Cranelift's x86_64 backend is that a WebAssembly address which is left-shifted by a constant amount from 1 to 3 will get folded into x86_64's addressing modes which perform shifts. For example `(i32.load (i32.shl (local.get 0) (i32.const 3)))` loads from the WebAssembly address `$local0 << 3`. When translated to Cranelift the `$local0 << 3` computation, a 32-bit value, is zero-extended to a 64-bit value and then added to the base address of linear memory. Cranelift would generate an instruction of the form `movl (%base, %local0, 8), %dst` which calculates `%base + %local0 << 3`. The bug here, however, is that the address computation happens with 64-bit values, where the `$local0 << 3` computation was supposed to be truncated to a a 32-bit value. This means that `%local0`, which can use up	9.9	More Details

CVE Number	Description	Base Score	Reference
26489	to 32-bits for an address, gets 3 extra bits of address space to be accessible via this `movl` instruction. The fix in Cranelift is to remove the erroneous lowering rules in the backend which handle these zero-extended expression. The above example is then translated to `movl %local0, %temp; shl $3, %temp; movl (%base, %temp), %dst` which correctly truncates the intermediate computation of `%local0 << 3` to 32-bits inside the `%temp` register which is then added to the `%base` value. Wasmtime version 4.0.1, 5.0.1, and 6.0.1 have been released and have all been patched to no longer contain the erroneous lowering rules. While updating Wasmtime is recommended, there are a number of possible workarounds that embedders can employ to mitigate this issue if updating is not possible. Note that none of these workarounds are on-by-default and require explicit configuration: 1. The `Config::static_memory_maximum_size(0)` option can be used to force all accesses to linear memory to be explicitly bounds-checked. This will perform a bounds check separately from the address-mode computation which correctly calculates the effective address of a load/store. Note that this can have a large impact on the execution performance of WebAssembly modules. 2. The `Config::static_memory_guard_size(1 << 36)` option can be used to greatly increase the guard pages placed after linear memory. This will guarantee that memory accesses up-to-34G away are guaranteed to be semantically correct by reserving unmapped memory for the instance. Note that this reserves a very large amount of virtual memory per-instances and can greatly reduce the maximum number of concurrent instances being run. 3. If using a non-x86_64 host is possible, then that will also work around this bug. This bug does not affect Wasmtime's or Cranelift's AArch64 backend, for example.		
CVE-2022-38074	SQL Injection vulnerability in VeronaLabs WP Statistics plugin <= 13.2.10 versions.	9.9	More Details
CVE-2023-23857	Due to missing authentication check, SAP NetWeaver AS for Java - version 7.50, allows an unauthenticated attacker to attach to an open interface and make use of an open naming and directory API to access services which can be used to perform unauthorized operations affecting users and services across systems. On a successful exploitation, the attacker can read and modify some sensitive information but can also be used to lock up any element or operation of the system making that it unresponsive or unavailable.	9.9	More Details
CVE-2023-25616	In some scenario, SAP Business Objects Business Intelligence Platform (CMC) - versions 420, 430, Program Object execution can lead to code injection vulnerability which could allow an attacker to gain access to resources that are allowed by extra privileges. Successful attack could highly impact the confidentiality, Integrity, and Availability of the system.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27063	Tenda V15V1.0 V15.11.0.14(1521_3190_1058) was discovered to contain a buffer overflow vulnerability via the DNSDomainName parameter in the formModifyDnsForward function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	9.8	More Details
CVE-2023-27061	Tenda V15V1.0 V15.11.0.14(1521_3190_1058) was discovered to contain a buffer overflow vulnerability via the wifiFilterListRemark parameter in the modifyWifiFilterRules function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	9.8	More Details
CVE-2023-24762	OS Command injection vulnerability in D-Link DIR-867 DIR_867_FW1.30B07 allows attackers to execute arbitrary commands via a crafted LocalIPAddress parameter for the SetVirtualServerSettings to HNAP1.	9.8	More Details
CVE-2023-24780	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the id parameter at /databases/table/columns.	9.8	More Details
CVE-2021-45423	A Buffer Overflow vulnerabilityexists in Pev 0.81 via the pe_exports function from exports.c.. The array offsets_to_Names is dynamically allocated on the stack using exp->NumberOfFunctions as its size. However, the loop uses exp->NumberOfNames to iterate over it and set its components value. Therefore, the loop code assumes that exp->NumberOfFunctions is greater than ordinal at each iteration. This can lead to arbitrary code execution.	9.8	More Details
CVE-2023-28154	Webpack 5 before 5.76.0 does not avoid cross-realm object access. ImportParserPlugin.js mishandles the magic comment feature. An attacker who controls a property of an untrusted object can obtain access to the real global object.	9.8	More Details
CVE-2022-48367	An issue was discovered in eZ Publish Ibexa Kernel before 7.5.28. Access control based on object state is mishandled.	9.8	More Details
CVE-2023-25143	An uncontrolled search path element vulnerability in the Trend Micro Apex One Server installer could allow an attacker to achieve a remote code execution state on affected products.	9.8	More Details
CVE-2023-1198	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saysis Starcities allows SQL Injection.This issue affects Starcities: through 1.3.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0090	The webservices in Proofpoint Enterprise Protection (PPS/POD) contain a vulnerability that allows for an anonymous user to execute remote code through 'eval injection'. Exploitation requires network access to the webservices API, but such access is a non-standard configuration. This affects all versions 8.20.0 and below.	9.8	More Details
CVE-2022-33256	Memory corruption due to improper validation of array index in Multi-mode call processor.	9.8	More Details
CVE-2023-0037	The 10Web Map Builder for Google Maps WordPress plugin before 1.0.73 does not properly sanitise and escape some parameters before using them in an SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection	9.8	More Details
CVE-2023-0345	The Akuvox E11 secure shell (SSH) server is enabled by default and can be accessed by the root user. This password cannot be changed by the user.	9.8	More Details
CVE-2023-25279	OS Command injection vulnerability in D-Link DIR820LA1_FW105B03 allows attackers to escalate privileges to root via a crafted payload.	9.8	More Details
CVE-2023-25207	PrestaShop dpdfrance <6.1.3 is vulnerable to SQL Injection via dpdfrance/ajax.php.	9.8	More Details
CVE-2023-27852	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 contains a buffer overflow vulnerability in various CGI mechanisms that could allow an attacker to execute arbitrary code on the device.	9.8	More Details
CVE-2023-27583	PanIndex is a network disk directory index. In Panindex prior to version 3.1.3, a hard-coded JWT key `PanIndex` is used. An attacker can use the hard-coded JWT key to sign JWT token and perform any actions as a user with admin privileges. Version 3.1.3 has a patch for the issue. As a workaround, one may change the JWT key in the source code before compiling the project.	9.8	More Details
CVE-2023-27052	E-Commerce System v1.0 ws discovered to contain a SQL injection vulnerability via the id parameter at /admin/delete_user.php.	9.8	More Details
CVE-2023-27074	BP Monitoring Management System v1.0 was discovered to contain a SQL injection vulnerability via the emailid parameter in the login page.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21708	Remote Procedure Call Runtime Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-23392	HTTP Protocol Stack Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-23397	Microsoft Outlook Elevation of Privilege Vulnerability	9.8	More Details
CVE-2023-23415	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-28343	OS command injection affects Altenergy Power Control Software C1.2.5 via shell metacharacters in the index.php/management/set_timezone timezone parameter, because of set_timezone in models/management_model.php.	9.8	More Details
CVE-2023-26511	A Hard Coded Admin Credentials issue in the Web-UI Admin Panel in Propius MachineSelector 6.6.0 and 6.6.1 allows remote attackers to gain access to the admin panel Propiusadmin.php, which allows taking control of the affected system.	9.8	More Details
CVE-2023-27853	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 contains a format string vulnerability in a SOAP service that could allow an attacker to execute arbitrary code on the device.	9.8	More Details
CVE-2023-1327	Netgear RAX30 (AX2400), prior to version 1.0.6.74, was affected by an authentication bypass vulnerability, allowing an unauthenticated attacker to gain administrative access to the device's web management interface by resetting the admin password.	9.8	More Details
CVE-2021-33360	An issue found in Stoqey gnuplot v.0.0.3 and earlier allows attackers to execute arbitrary code via the src/index.ts, plotCallack, child_process, and/or filePath parameter(s).	9.8	More Details
CVE-2023-22889	SmartBear Zephyr Enterprise through 7.15.0 mishandles user-defined input during report generation. This could lead to remote code execution by unauthenticated users.	9.8	More Details
CVE-2023-26922	SQL injection vulnerability found in Varisicte matrix-gui v.2 allows a remote attacker to execute arbitrary code via the shell_exect parameter to the \www\pages\matrix-gui-2.0 endpoint.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24782	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the id parameter at /databases/database/edit.	9.8	More Details
CVE-2023-24773	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the id parameter at /databases/database/list.	9.8	More Details
CVE-2023-26261	In UBIKA WAAP Gateway/Cloud through 6.10, a blind XPath injection leads to an authentication bypass by stealing the session of another connected user. The fixed versions are WAAP Gateway & Cloud 6.11.0 and 6.5.6-patch15.	9.8	More Details
CVE-2021-33352	An issue in Wyomind Help Desk Magento 2 extension v.1.3.6 and before fixed in v.1.3.7 allows attacker to execute arbitrary code via a phar file upload in the ticket message field.	9.8	More Details
CVE-2021-33353	Directory Traversal vulnerability in Wyomind Help Desk Magento 2 extension v.1.3.6 and before fixed in v.1.3.7 allows attacker to execute arbitrary code via the file attachment directory setting.	9.8	More Details
CVE-2023-24774	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the selectFields parameter at \controller\auth\Auth.php.	9.8	More Details
CVE-2023-25395	TOTOlink A7100RU V7.4cu.2313_B20191024 router was discovered to contain a command injection vulnerability via the ou parameter at /setting/delStaticDhcpRules.	9.8	More Details
CVE-2023-24777	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the id parameter at /databases/table/list.	9.8	More Details
CVE-2023-1251	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Akinsoft Wolvox. This issue affects Wolvox: before 8.02.03.	9.8	More Details
CVE-2023-1267	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ulkem Company PtteM Kart.This issue affects PtteM Kart: before 2.1.	9.8	More Details
CVE-2023-1269	Use of Hard-coded Credentials in GitHub repository alextselegidis/easyappointments prior to 1.5.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27202	Best POS Management System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /kruxton/receipt.php.	9.8	More Details
CVE-2023-27203	Best POS Management System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /billing/home.php.	9.8	More Details
CVE-2023-27204	Best POS Management System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /kruxton/manage_user.php.	9.8	More Details
CVE-2023-27205	Best POS Management System 1.0 was discovered to contain a SQL injection vulnerability via the month parameter at /kruxton/sales_report.php.	9.8	More Details
CVE-2023-27207	Online Pizza Ordering System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/manage_user.php.	9.8	More Details
CVE-2023-27210	Online Pizza Ordering System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/view_order.php.	9.8	More Details
CVE-2023-27213	Online Student Management System v1.0 was discovered to contain a SQL injection vulnerability via the searchdata parameter at /eduauth/student/search.php.	9.8	More Details
CVE-2023-27214	Online Student Management System v1.0 was discovered to contain multiple SQL injection vulnerabilities via the fromdate and todate parameters at /eduauth/student/between-date-reprtsdetails.php.	9.8	More Details
CVE-2023-1307	Authentication Bypass by Primary Weakness in GitHub repository froxlor/froxlor prior to 2.0.13.	9.8	More Details
CVE-2023-1091	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Alpata Licensed Warehousing Automation System allows Command Line Execution through SQL Injection.This issue affects Licensed Warehousing Automation System: through 2023.1.01.	9.8	More Details
CVE-2023-27905	Jenkins update-center2 3.13 and 3.14 renders the required Jenkins core version on plugin download index pages without sanitization, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide a plugin for hosting.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27898	Jenkins 2.270 through 2.393 (both inclusive), LTS 2.277.1 through 2.375.3 (both inclusive) does not escape the Jenkins version a plugin depends on when rendering the error message stating its incompatibility with the current version of Jenkins, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide plugins to the configured update sites and have this message shown by Jenkins instances.	9.6	More Details
CVE-2023-27269	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable.	9.6	More Details
CVE-2023-27500	An attacker with non-administrative authorizations can exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written making the system unavailable.	9.6	More Details
CVE-2022-39214	Combodo iTop is an open source, web-based IT service management platform. Prior to versions 2.7.8 and 3.0.2-1, a user who can log in on iTop is able to take over any account just by knowing the account's username. This issue is fixed in versions 2.7.8 and 3.0.2-1.	9.6	More Details
CVE-2022-33257	Memory corruption in Core due to time-of-check time-of-use race condition during dump collection in trust zone.	9.3	More Details
CVE-2023-25957	A vulnerability has been identified in Mendix SAML (Mendix 7 compatible) (All versions >= V1.16.4 < V1.17.3), Mendix SAML (Mendix 8 compatible) (All versions >= V2.2.0 < V2.3.0), Mendix SAML (Mendix 9 latest compatible, New Track) (All versions >= V3.1.9 < V3.3.1), Mendix SAML (Mendix 9 latest compatible, Upgrade Track) (All versions >= V3.1.8 < V3.3.0), Mendix SAML (Mendix 9.6 compatible, New Track) (All versions >= V3.1.9 < V3.2.7), Mendix SAML (Mendix 9.6 compatible, Upgrade Track) (All versions >= V3.1.8 < V3.2.6). The affected versions of the module insufficiently verify the SAML assertions. This could allow unauthenticated remote attackers to bypass authentication and get access to the application. For compatibility reasons, fix versions still contain this issue, but only when the recommended, default configuration option `'Use Encryption'` is disabled.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27582	maddy is a composable, all-in-one mail server. Starting with version 0.2.0 and prior to version 0.6.3, maddy allows a full authentication bypass if SASL authorization username is specified when using the PLAIN authentication mechanisms. Instead of validating the specified username, it is accepted as is after checking the credentials for the authentication username. maddy 0.6.3 includes the fix for the bug. There are no known workarounds.	9.1	More Details
CVE-2023-0352	The Akuvox E11 password recovery webpage can be accessed without authentication, and an attacker could download the device key file. An attacker could then use this page to reset the password back to the default.	9.1	More Details
CVE-2023-26957	onekeyadmin v1.3.9 was discovered to contain an arbitrary file delete vulnerability via the component \admin\controller\plugins.	9.1	More Details
CVE-2023-0354	The Akuvox E11 web server can be accessed without any user authentication, and this could allow an attacker to access sensitive information, as well as create and download packet captures with known default URLs.	9.1	More Details
CVE-2023-25617	SAP Business Object (Adaptive Job Server) - versions 420, 430, allows remote execution of arbitrary commands on Unix, when program objects execution is enabled, to authenticated users with scheduling rights, using the BI Launchpad, Central Management Console or a custom application based on the public java SDK. Programs could impact the confidentiality, integrity and availability of the system.	9.0	More Details
CVE-2021-33351	Cross Site Scripting Vulnerability in Wyomind Help Desk Magento 2 extension v.1.3.6 and before and fixed in v.1.3.7 allows attackers to escalte privileges via a crafted payload in the ticket message field.	9.0	More Details
CVE-2023-1287	An XSL template vulnerability in ENOVIA Live Collaboration V6R2013xE allows Remote Code Execution.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-1313	Unrestricted Upload of File with Dangerous Type in GitHub repository cockpit-hq/cockpit prior to 2.4.1.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24871	Windows Bluetooth Service Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-23403	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-27893	An attacker authenticated as a user with a non-administrative role and a common remote execution authorization in SAP Solution Manager and ABAP managed systems (ST-PI) - versions 2088_1_700, 2008_1_710, 740, can use a vulnerable interface to execute an application function to perform actions which they would not normally be permitted to perform. Depending on the function executed, the attack can read or modify any user or application data and can make the application unavailable.	8.8	More Details
CVE-2023-23406	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-27581	github-slug-action is a GitHub Action to expose slug value of GitHub environment variables inside of one's GitHub workflow. Starting in version 4.0.0` and prior to version 4.4.1, this action uses the `github.head_ref` parameter in an insecure way. This vulnerability can be triggered by any user on GitHub on any workflow using the action on pull requests. They just need to create a pull request with a branch name, which can contain the attack payload. This can be used to execute code on the GitHub runners and to exfiltrate any secrets one uses in the CI pipeline. A patched action is available in version 4.4.1. No workaround is available.	8.8	More Details
CVE-2023-0351	The Akuvox E11 web server backend library allows command injection in the device phone-book contacts functionality. This could allow an attacker to upload files with executable command instructions.	8.8	More Details
CVE-2023-23413	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-0477	The Auto Featured Image (Auto Post Thumbnail) WordPress plugin before 3.9.16 includes an AJAX endpoint that allows any user with at least Author privileges to upload arbitrary files, such as PHP files. This is caused by incorrect file extension validation.	8.8	More Details
CVE-2023-0089	The webutils in Proofpoint Enterprise Protection (PPS/POD) contain a vulnerability that allows an authenticated user to execute remote code through 'eval injection'. This affects all versions 8.20.0 and below.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23328	A File Upload vulnerability exists in AvantFAX 3.3.7. An authenticated user can bypass PHP file type validation in FileUpload.php by uploading a specially crafted PHP file.	8.8	More Details
CVE-2023-24864	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability	8.8	More Details
CVE-2023-23388	Windows Bluetooth Driver Elevation of Privilege Vulnerability	8.8	More Details
CVE-2023-24868	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-24867	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-24872	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-24909	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-28339	OpenDoas through 6.8.2, when TIOCSTI is available, allows privilege escalation because of sharing a terminal with the original session. NOTE: TIOCSTI is unavailable in OpenBSD 6.0 and later, and can be made unavailable in the Linux kernel 6.2 and later.	8.8	More Details
CVE-2023-25206	PrestaShop ws_productreviews < 3.6.2 is vulnerable to SQL Injection.	8.8	More Details
CVE-2023-1205	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 is vulnerable to cross-site request forgery attacks on all endpoints due to improperly implemented CSRF protections.	8.8	More Details
CVE-2023-24913	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27851	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 contains a file sharing mechanism that unintentionally allows users with upload permissions to execute arbitrary code on the device.	8.8	More Details
CVE-2023-27088	feiqu-opensource Background Vertical authorization vulnerability exists in IndexController.java. demo users with low permission can perform operations within the permission of the admin super administrator and can use this vulnerability to change the blacklist IP address in the system at will.	8.8	More Details
CVE-2022-46394	An issue was discovered in the Arm Mali GPU Kernel Driver. A non-privileged user can make improper GPU processing operations to gain access to already freed memory. This affects Valhall r39p0 through r41p0 before r42p0, and Avalon r41p0 before r42p0.	8.8	More Details
CVE-2023-24907	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-24876	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-27463	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.3). The audit log form of affected applications is vulnerable to SQL injection. This could allow authenticated remote attackers to execute arbitrary SQL queries on the server database.	8.8	More Details
CVE-2023-0050	An issue has been discovered in GitLab affecting all versions starting from 13.7 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. A specially crafted Kroki diagram could lead to a stored XSS on the client side which allows attackers to perform arbitrary actions on behalf of victims.	8.7	More Details
CVE-2023-27501	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a directory traversal flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20049	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads.	8.6	More Details
CVE-2023-25573	metersphere is an open source continuous testing platform. In affected versions an improper access control vulnerability exists in `/api/jmeter/download/files`, which allows any user to download any file without authentication. This issue may expose all files available to the running process. This issue has been addressed in version 1.20.20 lts and 2.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.6	More Details
CVE-2022-40539	Memory corruption in Automotive Android OS due to improper validation of array index.	8.4	More Details
CVE-2022-40540	Memory corruption due to buffer copy without checking the size of input while loading firmware in Linux Kernel.	8.4	More Details
CVE-2022-25694	Memory corruption in Modem due to usage of Out-of-range pointer offset in UIM	8.4	More Details
CVE-2022-40531	Memory corruption in WLAN due to incorrect type cast while sending WMI_SCAN_SCH_PRIO_TBL_CMDID message.	8.4	More Details
CVE-2022-40530	Memory corruption in WLAN due to integer overflow to buffer overflow in WLAN during initialization phase.	8.4	More Details
CVE-2022-25655	Memory corruption in WLAN HAL while arbitrary value is passed in WMI UTF command payload.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25709	Memory corruption in modem due to use of out of range pointer offset while processing qmi msg	8.4	More Details
CVE-2021-27788	HCL Verse is susceptible to a Cross Site Scripting (XSS) vulnerability. By tricking a user into clicking a crafted URL, a remote unauthenticated attacker could execute script in a victim's web browser to perform operations as the victim and/or steal the victim's cookies, session tokens, or other sensitive information.	8.3	More Details
CVE-2023-27476	OWSLib is a Python package for client programming with Open Geospatial Consortium (OGC) web service interface standards, and their related content models. OWSLib's XML parser (which supports both `lxml` and `xml.etree`) does not disable entity resolution, and could lead to arbitrary file reads from an attacker-controlled XML payload. This affects all XML parsing in the codebase. This issue has been addressed in version 0.28.1. All users are advised to upgrade. The only known workaround is to patch the library manually. See `GHSA-8h9c-r582-mggc` for details.	8.2	More Details
CVE-2023-23383	Service Fabric Explorer Spoofing Vulnerability	8.2	More Details
CVE-2023-24892	Microsoft Edge (Chromium-based) Webview2 Spoofing Vulnerability	8.2	More Details
CVE-2023-23404	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-24908	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27486	xCAT is a toolkit for deployment and administration of computer clusters. In versions prior to 2.16.5 if zones are configured as a mechanism to secure clusters in XCAT, it is possible for a local root user from one node to obtain credentials to SSH to any node in any zone, except the management node of the default zone. XCAT zones are not enabled by default. Only users that use the optional zone feature are impacted. All versions of xCAT prior to xCAT 2.16.5 are vulnerable. This problem has been fixed in xCAT 2.16.5. Users making use of zones should upgrade to 2.16.5. Users unable to upgrade may mitigate the issue by disabling zones or patching the management node with the fix contained in commit `85149c37f49`.	8.1	More Details
CVE-2023-24869	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-22891	There exists a privilege escalation vulnerability in SmartBear Zephyr Enterprise through 7.15.0 that could be exploited by authorized users to reset passwords for other accounts.	8.1	More Details
CVE-2023-23405	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-27490	NextAuth.js is an open source authentication solution for Next.js applications. `next-auth` applications using OAuth provider versions before `v4.20.1` have been found to be subject to an authentication vulnerability. A bad actor who can read traffic on the victim's network or who is able to social engineer the victim to click a manipulated login link could intercept and tamper with the authorization URL to **log in as the victim**, bypassing the CSRF protection. This is due to a partial failure during a compromised OAuth session where a session code is erroneously generated. This issue has been addressed in version 4.20.1. Users are advised to upgrade. Users unable to upgrade may using Advanced Initialization, manually check the callback request for state, pkce, and nonce against the provider configuration to prevent this issue. See the linked GHSA for details.	8.1	More Details
CVE-2023-27401	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20308, ZDI-CAN-20345)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27404	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application is vulnerable to stack-based buffer while parsing specially crafted SPP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-20433)	7.8	More Details
CVE-2023-23421	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-23422	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-23423	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-33278	Memory corruption due to buffer copy without checking the size of input in HLOS when input message size is larger than the buffer capacity.	7.8	More Details
CVE-2023-23402	Windows Media Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-33242	Memory corruption due to improper authentication in Qualcomm IPC while loading unsigned lib in audio PD.	7.8	More Details
CVE-2022-25705	Memory corruption in modem due to integer overflow to buffer overflow while handling APDU response	7.8	More Details
CVE-2023-27400	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-20300)	7.8	More Details
CVE-2023-27405	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20432)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27406	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application is vulnerable to stack-based buffer while parsing specially crafted SPP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-20449)	7.8	More Details
CVE-2022-20929	A vulnerability in the upgrade signature verification of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an unauthenticated, local attacker to provide an unauthentic upgrade file for upload. This vulnerability is due to insufficient cryptographic signature verification of upgrade files. An attacker could exploit this vulnerability by providing an administrator with an unauthentic upgrade file. A successful exploit could allow the attacker to fully compromise the Cisco NFVIS system.	7.8	More Details
CVE-2023-23401	Windows Media Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-24910	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-24930	Microsoft OneDrive for MacOS Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-23420	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-25144	An improper access control vulnerability in the Trend Micro Apex One agent could allow a local attacker to gain elevated privileges and create arbitrary directories with arbitrary ownership.	7.8	More Details
CVE-2023-25145	A link following vulnerability in the scanning function of Trend Micro Apex One agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2023-25146	A security agent link following vulnerability in the Trend Micro Apex One agent could allow a local attacker to quarantine a file, delete the original folder and replace with a junction to an arbitrary location, ultimately leading to an arbitrary file dropped to an arbitrary location. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23419	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-25148	A security agent link following vulnerability in Trend Micro Apex One could allow a local attacker to exploit the vulnerability by changing a specific file into a pseudo-symlink, allowing privilege escalation on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2023-22436	The kernel subsystem function check_permission_for_set_tokenid within OpenHarmony-v3.1.5 and prior versions has an UAF vulnerability which local attackers can exploit this vulnerability to escalate the privilege to root.	7.8	More Details
CVE-2023-23418	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-23417	Windows Partition Management Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-23416	Windows Cryptographic Services Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-27010	Wondershare Dr.Fone v12.9.6 was discovered to contain weak permissions for the service WsDrvInst. This vulnerability allows attackers to escalate privileges via modifying or overwriting the executable.	7.8	More Details
CVE-2023-23412	Windows Accounts Picture Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-23410	Windows HTTP.sys Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-27403	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains a memory corruption vulnerability while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20303, ZDI-CAN-20348)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27402	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20334)	7.8	More Details
CVE-2023-27398	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-20304)	7.8	More Details
CVE-2023-27399	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-20299, ZDI-CAN-20346)	7.8	More Details
CVE-2023-23399	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-27590	Rizin is a UNIX-like reverse engineering framework and command-line toolset. In version 0.5.1 and prior, converting a GDB registers profile file into a Rizin register profile can result in a stack-based buffer overflow when the `name`, `type`, or `groups` fields have longer values than expected. Users opening untrusted GDB registers files (e.g. with the `drpg` or `arpg` commands) are affected by this flaw. Commit d6196703d89c84467b600ba2692534579dc25ed4 contains a patch for this issue. As a workaround, review the GDB register profiles before loading them with `drpg`/`arpg` commands.	7.8	More Details
CVE-2023-0030	A use-after-free flaw was found in the Linux kernel's nouveau driver in how a user triggers a memory overflow that causes the nvkm_vma_tail function to fail. This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.8	More Details
CVE-2023-27986	emacsclient-mail.desktop in Emacs 28.1 through 28.2 is vulnerable to Emacs Lisp code injections through a crafted mailto: URI with unescaped double-quote characters. It is fixed in 29.0.90.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0622	Cscape Envision RV version 4.60 is vulnerable to an out-of-bounds write vulnerability when parsing project (i.e. HMI) files. The product lacks proper validation of user-supplied data, which could result in writes past the end of allocated data structures. An attacker could leverage these vulnerabilities to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2023-0621	Cscape Envision RV version 4.60 is vulnerable to an out-of-bounds read vulnerability when parsing project (i.e. HMI) files. The product lacks proper validation of user-supplied data, which could result in reads past the end of allocated data structures. An attacker could leverage these vulnerabilities to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2023-1277	A vulnerability, which was classified as critical, was found in kylin-system-updater up to 1.4.20kord on Ubuntu Kylin. Affected is the function InstallSnap of the component Update Handler. The manipulation leads to command injection. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222600.	7.8	More Details
CVE-2023-27985	emacsclient-mail.desktop in Emacs 28.1 through 28.2 is vulnerable to shell command injections through a crafted mailto: URI. This is related to lack of compliance with the Desktop Entry Specification. It is fixed in 29.0.90	7.8	More Details
CVE-2023-27117	WebAssembly v1.0.29 was discovered to contain a heap overflow via the component component wabt::Node::operator.	7.8	More Details
CVE-2023-0623	Cscape Envision RV version 4.60 is vulnerable to an out-of-bounds write vulnerability when parsing project (i.e. HMI) files. The product lacks proper validation of user-supplied data, which could result in writes past the end of allocated data structures. An attacker could leverage these vulnerabilities to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2022-3767	Missing validation in DAST analyzer affecting all versions from 1.11.0 prior to 3.0.32, allows custom request headers to be sent with every request, regardless of the host.	7.7	More Details
CVE-2023-26076	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G SM message codec can occur due to insufficient parameter validation when decoding reserved options.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26072	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list.	7.6	More Details
CVE-2023-26073	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list.	7.6	More Details
CVE-2023-26075	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List.	7.6	More Details
CVE-2023-26074	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions.	7.6	More Details
CVE-2023-0346	Akuvox E11 cloud login is performed through an unencrypted HTTP connection. An attacker could gain access to the Akuvox cloud and device if the MAC address of a device if known.	7.5	More Details
CVE-2021-34125	An issue discovered in Yuneec Mantis Q and PX4-Autopilot v 1.11.3 and below allow attacker to gain access to sensitive information via various nuttx commands.	7.5	More Details
CVE-2023-24858	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	7.5	More Details
CVE-2023-0349	The Akuvox E11 libvoice library provides unauthenticated access to the camera capture for image and video. This could allow an attacker to view and record image and video from the camera.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24856	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	7.5	More Details
CVE-2021-33639	REMAP cmd of SVM driver can be used to remap read only memory as read-write, then cause read only memory/file modified.	7.5	More Details
CVE-2018-25081	Bitwarden through 2023.2.1 offers password auto-fill within a cross-domain IFRAME element. NOTE: the vendor's position is that there have been important legitimate cross-domain configurations (e.g., an apple.com IFRAME element on the icloud.com website) and that "Auto-fill on page load" is not enabled by default.	7.5	More Details
CVE-2023-27974	Bitwarden through 2023.2.1 offers password auto-fill when the second-level domain matches, e.g., a password stored for an example.com hosting provider when customer-website.example.com is visited. NOTE: the vendor's position is that "Auto-fill on page load" is not enabled by default.	7.5	More Details
CVE-2023-25802	Roxy-WI is a Web interface for managing Haproxy, Nginx, Apache, and Keepalived servers. Versions prior to 6.3.6.0 don't correctly neutralize `dir/../filename` sequences, such as `/etc/nginx/../passwd`, allowing an actor to gain information about a server. Version 6.3.6.0 has a patch for this issue.	7.5	More Details
CVE-2023-26948	onekeyadmin v1.3.9 was discovered to contain an arbitrary file read vulnerability via the component /admin1/file/download.	7.5	More Details
CVE-2023-1246	Files or Directories Accessible to External Parties vulnerability in Saysis Starcities allows Collect Data from Common Resource Locations.This issue affects Starcities: through 1.3.	7.5	More Details
CVE-2023-0347	The Akuvox E11 Media Access Control (MAC) address, a primary identifier, combined with the Akuvox E11 IP address, could allow an attacker to identify the device on the Akuvox cloud.	7.5	More Details
CVE-2022-33213	Memory corruption in modem due to buffer overflow while processing a PPP packet	7.5	More Details
CVE-2022-33244	Transient DOS due to reachable assertion in modem during MIB reception and SIB timeout	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0348	Akuvox E11 allows direct SIP calls. No access control is enforced by the SIP servers, which could allow an attacker to contact any device within Akuvox to call any other device.	7.5	More Details
CVE-2023-24859	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability	7.5	More Details
CVE-2022-33254	Transient DOS due to reachable assertion in Modem while processing SIB1 Message.	7.5	More Details
CVE-2023-25803	Roxy-WI is a Web interface for managing Haproxy, Nginx, Apache, and Keepalived servers. Versions prior to 6.3.5.0 have a directory traversal vulnerability that allows the inclusion of server-side files. This issue is fixed in version 6.3.5.0.	7.5	More Details
CVE-2022-33272	Transient DOS in modem due to reachable assertion.	7.5	More Details
CVE-2022-40527	Transient DOS due to reachable assertion in WLAN while processing PEER ID populated by TQM.	7.5	More Details
CVE-2023-25283	A stack overflow vulnerability in D-Link DIR820LA1_FW106B02 allows attackers to cause a denial of service via the reserveDHCP_HostName_1.1.1.0 parameter to lan.asp.	7.5	More Details
CVE-2022-40535	Transient DOS due to buffer over-read in WLAN while sending a packet to device.	7.5	More Details
CVE-2023-24033	The Samsung Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets do not properly check format types specified by the Session Description Protocol (SDP) module, which can lead to a denial of service.	7.5	More Details
CVE-2022-33250	Transient DOS due to reachable assertion in modem when network repeatedly sent invalid message container for NR to LTE handover.	7.5	More Details
CVE-2022-33309	Transient DOS due to buffer over-read in WLAN Firmware while parsing secure FTMR frame with size lesser than 39 Bytes.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27585	PJSIP is a free and open source multimedia communication library written in C. A buffer overflow vulnerability in versions 2.13 and prior affects applications that use PJSIP DNS resolver. It doesn't affect PJSIP users who do not utilise PJSIP DNS resolver. This vulnerability is related to CVE-2022-24793. The difference is that this issue is in parsing the query record `parse_query()`, while the issue in CVE-2022-24793 is in `parse_rr()`. A patch is available as commit `d1c5e4d` in the `master` branch. A workaround is to disable DNS resolution in PJSIP config (by setting `nameserver_count` to zero) or use an external resolver implementation instead.	7.5	More Details
CVE-2023-27161	Jellyfin up to v10.7.7 was discovered to contain a Server-Side Request Forgery (SSRF) via the component /Repositories. This vulnerability allows attackers to access network resources and sensitive information via a crafted POST request.	7.5	More Details
CVE-2023-27530	A DoS vulnerability exists in Rack <v3.0.4.2, <v2.2.6.3, <v2.1.4.3 and <v2.0.9.3 within in the Multipart MIME parsing code in which could allow an attacker to craft requests that can be abuse to cause multipart parsing to take longer than expected.	7.5	More Details
CVE-2023-23911	An improper access control vulnerability exists prior to v6 that could allow an attacker to break the E2E encryption of a chat room by a user changing the group key of a chat room.	7.5	More Details
CVE-2023-27065	Tenda V15V1.0 V15.11.0.14(1521_3190_1058) was discovered to contain a buffer overflow vulnerability via the picName parameter in the formDelWewifiPi function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2023-27588	Hasura is an open-source product that provides users GraphQL or REST APIs. A path traversal vulnerability has been discovered within Hasura GraphQL Engine prior to versions 1.3.4, 2.55.1, 2.20.1, and 2.21.0-beta1. Projects running on Hasura Cloud were not vulnerable. Self-hosted Hasura Projects with deployments that are publicly exposed and not protected by a WAF or other HTTP protection layer should be upgraded to version 1.3.4, 2.55.1, 2.20.1, or 2.21.0-beta1 to receive a patch.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26464	** UNSUPPORTED WHEN ASSIGNED ** When using the Chainsaw or SocketAppender components with Log4j 1.x on JRE less than 1.7, an attacker that manages to cause a logging entry involving a specially-crafted (ie, deeply nested) hashmap or hashtable (depending on which logging component is in use) to be processed could exhaust the available memory in the virtual machine and achieve Denial of Service when the object is deserialized. This issue affects Apache Log4j before 2. Affected users are recommended to update to Log4j 2.x. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	7.5	More Details
CVE-2023-27064	Tenda V15V1.0 V15.11.0.14(1521_3190_1058) was discovered to contain a buffer overflow vulnerability via the index parameter in the formDelDnsForward function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2023-22892	There exists an information disclosure vulnerability in SmartBear Zephyr Enterprise through 7.15.0 that could be exploited by unauthenticated users to read arbitrary files from Zephyr instances.	7.5	More Details
CVE-2023-27062	Tenda V15V1.0 was discovered to contain a buffer overflow vulnerability via the gotoUrl parameter in the formPortalAuth function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2022-44574	An improper authentication vulnerability exists in Avalanche version 6.3.x and below allows unauthenticated attacker to modify properties on specific port.	7.5	More Details
CVE-2023-27580	CodeIgniter Shield provides authentication and authorization for the CodeIgniter 4 PHP framework. An improper implementation was found in the password storage process. All hashed passwords stored in Shield v1.0.0-beta.3 or earlier are easier to crack than expected due to the vulnerability. Therefore, they should be removed as soon as possible. If an attacker gets (1) the user's hashed password by Shield, and (2) the hashed password (SHA-384 hash without salt) from somewhere, the attacker may easily crack the user's password. Upgrade to Shield v1.0.0-beta.4 or later to fix this issue. After upgrading, all users' hashed passwords should be updated (saved to the database). There are no known workarounds.	7.5	More Details
CVE-2022-31474	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in iThemes BackupBuddy allows Path Traversal.This issue affects BackupBuddy: from 8.5.8.0 through 8.7.4.1.	7.5	More Details
CVE-2023-27532	Vulnerability in Veeam Backup & Replication component allows encrypted credentials stored in the configuration database to be obtained. This may lead to gaining access to the backup infrastructure hosts.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27901	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier uses the Apache Commons FileUpload library without specifying limits for the number of request parts introduced in version 1.5 for CVE-2023-24998 in org.kohsuke.stapler.RequestImpl, allowing attackers to trigger a denial of service.	7.5	More Details
CVE-2023-26956	onekeyadmin v1.3.9 was discovered to contain an arbitrary file read vulnerability via the component /admin1/curd/code.	7.5	More Details
CVE-2023-27900	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier uses the Apache Commons FileUpload library without specifying limits for the number of request parts introduced in version 1.5 for CVE-2023-24998 in hudson.util.MultipartFormDataParser, allowing attackers to trigger a denial of service.	7.5	More Details
CVE-2023-22890	SmartBear Zephyr Enterprise through 7.15.0 allows unauthenticated users to upload large files, which could exhaust the local drive space, causing a denial of service condition.	7.5	More Details
CVE-2023-24533	Multiplication of certain unreduced P-256 scalars produce incorrect results. There are no protocols known at this time that can be attacked due to this.	7.5	More Details
CVE-2023-27587	ReadtoMyShoe, a web app that lets users upload articles and listen to them later, generates an error message containing sensitive information prior to commit 8533b01. If an error occurs when adding an article, the website shows the user an error message. If the error originates from the Google Cloud TTS request, then it will include the full URL of the request. The request URL contains the Google Cloud API key. This has been patched in commit 8533b01. Upgrading should be accompanied by deleting the current GCP API key and issuing a new one. There are no known workarounds.	7.4	More Details
CVE-2022-39216	Combodo iTop is an open source, web-based IT service management platform. Prior to versions 2.7.8 and 3.0.2-1, the reset password token is generated without any randomness parameter. This may lead to account takeover. The issue is fixed in versions 2.7.8 and 3.0.2-1.	7.4	More Details
CVE-2023-1299	HashiCorp Nomad and Nomad Enterprise 1.5.0 allow a job submitter to escalate to management-level privileges using workload identity and task API. Fixed in 1.5.1.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26459	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability.	7.4	More Details
CVE-2023-1368	A vulnerability was found in XHCMS 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php of the component POST Parameter Handler. The manipulation of the argument user leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-222874 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2023-1365	A vulnerability was found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/ajax.php. The manipulation of the argument username leads to sql injection. 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-222872.	7.3	More Details
CVE-2023-1357	A vulnerability, which was classified as critical, has been found in SourceCodester Simple Bakery Shop Management System 1.0. Affected by this issue is some unknown functionality of the component Admin Login. The manipulation of the argument username/password with the input admin' or 1=1 -- leads to sql injection. 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-222860.	7.3	More Details
CVE-2022-40537	Memory corruption in Bluetooth HOST while processing the AVRC_PDU_GET_PLAYER_APP_VALUE_TEXT AVRCP response.	7.3	More Details
CVE-2023-1294	A vulnerability was found in SourceCodester File Tracker Manager System 1.0. It has been classified as critical. Affected is an unknown function of the file /file_manager/login.php of the component POST Parameter Handler. 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-222648.	7.3	More Details
CVE-2023-26109	All versions of the package node-bluetooth-serial-port are vulnerable to Buffer Overflow via the findSerialPortChannel method due to improper user input length validation.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26110	All versions of the package node-bluetooth are vulnerable to Buffer Overflow via the findSerialPortChannel method due to improper user input length validation.	7.3	More Details
CVE-2022-40515	Memory corruption in Video due to double free while playing 3gp clip with invalid metadata atoms.	7.3	More Details
CVE-2023-23400	Windows DNS Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2023-27498	SAP Host Agent (SAPOSCOL) - version 7.22, allows an unauthenticated attacker with network access to a server port assigned to the SAP Start Service to submit a crafted request which results in a memory corruption error. This error can be used to reveal but not modify any technical information about the server. It can also make a particular service temporarily unavailable	7.2	More Details
CVE-2023-1372	The WH Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several parameters such as wh_homepage, wh_text_short, wh_text_full and in versions up to, and including, 3.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2022-48365	An issue was discovered in eZ Platform Ibexa Kernel before 1.3.26. The Company admin role gives excessive privileges.	7.2	More Details
CVE-2023-0353	Akuvox E11 uses a weak encryption algorithm for stored passwords and uses a hard-coded password for decryption which could allow the encrypted passwords to be decrypted from the configuration file.	7.2	More Details
CVE-2023-26262	An issue was discovered in Sitecore XP/XM 10.3. As an authenticated Sitecore user, a unrestricted language file upload vulnerability exists the can lead to direct code execution on the content management (CM) server.	7.2	More Details
CVE-2023-23398	Microsoft Excel Spoofing Vulnerability	7.1	More Details
CVE-2023-23407	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0629	Docker Desktop before 4.17.0 allows an unprivileged user to bypass Enhanced Container Isolation (ECI) restrictions by setting the Docker host to docker.raw.sock, or npipe:////.pipe/docker_engine_linux on Windows, via the -H (--host) CLI flag or the DOCKER_HOST environment variable and launch containers without the additional hardening features provided by ECI. This would not affect already running containers, nor containers launched through the usual approach (without Docker's raw socket). The affected functionality is available for Docker Business customers only and assumes an environment where users are not granted local root or Administrator privileges. This issue has been fixed in Docker Desktop 4.17.0. Affected Docker Desktop versions: from 4.13.0 before 4.17.0.	7.1	More Details
CVE-2023-23414	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability	7.1	More Details
CVE-2023-25814	metersphere is an open source continuous testing platform. In versions prior to 2.7.1 a user who has permission to create a resource file through UI operations is able to append a path to their submission query which will be read by the system and displayed to the user. This allows a users of the system to read arbitrary files on the filesystem of the server so long as the server process itself has permission to read the requested files. This issue has been addressed in version 2.7.1. All users are advised to upgrade. There are no known workarounds for this issue.	7.1	More Details
CVE-2023-23393	Windows BrokerInfrastructure Service Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-24861	Windows Graphics Component Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-28144	KDAB Hotspot 1.3.x and 1.4.x through 1.4.1, in a non-default configuration, allows privilege escalation because of race conditions involving symlinks and elevate_perf_privileges.sh chown calls.	7.0	More Details
CVE-2023-27899	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier creates a temporary file in the default temporary directory with the default permissions for newly created files when uploading a plugin for installation, potentially allowing attackers with access to the Jenkins controller file system to read and write the file before it is used, potentially resulting in arbitrary code execution.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23385	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-1288	An XML External Entity injection (XXE) vulnerability in ENOVIA Live Collaboration V6R2013xE allows an attacker to read local files on the server.	6.8	More Details
CVE-2023-25615	Due to insufficient input sanitization, SAP ABAP - versions 751, 753, 753, 754, 756, 757, 791, allows an authenticated high privileged user to alter the current session of the user by injecting the malicious database queries over the network and gain access to the unintended data. This may lead to a high impact on the confidentiality and no impact on the availability and integrity of the application.	6.8	More Details
CVE-2023-26461	SAP NetWeaver allows (SAP Enterprise Portal) - version 7.50, allows an authenticated attacker with sufficient privileges to access the XML parser which can submit a crafted XML file which when parsed will enable them to access but not modify sensitive files and data. It allows the attacker to view sensitive data which is owned by certain privileges.	6.8	More Details
CVE-2023-27850	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 contains a file sharing mechanism that allows users with access to this feature to access arbitrary files on the device.	6.8	More Details
CVE-2022-47462	In telephone service, there is a missing permission check. This could lead to local escalation of privilege with system execution privileges needed.	6.7	More Details
CVE-2022-33245	Memory corruption in WLAN due to use after free	6.7	More Details
CVE-2023-25147	An issue in the Trend Micro Apex One agent could allow an attacker who has previously acquired administrative rights via other means to bypass the protection by using a specifically crafted DLL during a specific update process. Please note: an attacker must first obtain administrative access on the target system via another method in order to exploit this.	6.7	More Details
CVE-2022-47461	In telephone service, 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-2023-27577	flarum is a forum software package for building communities. In versions prior to 1.7.0 an admin account which has already been compromised by an attacker may use a vulnerability in the `LESS` parser which can be exploited to read sensitive files on the server through the use of path traversal techniques. An attacker can achieve this by providing an absolute path to a sensitive file in the custom `LESS` setting, which the `LESS` parser will then read. For example, an attacker could use the following code to read the contents of the `/etc/passwd` file on a linux machine. The scope of what files are vulnerable will depend on the permissions given to the running flarum process. The vulnerability has been addressed in version `1.7`. Users should upgrade to this version to mitigate the vulnerability. Users unable to upgrade may mitigate the vulnerability by ensuring that their admin accounts are secured with strong passwords and follow other best practices for account security. Additionally, users can limit the exposure of sensitive files on the server by implementing appropriate file permissions and access controls at the operating system level.	6.6	More Details
CVE-2023-27310	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.2). The client query handler of the affected application fails to check for proper permissions when assigning groups to user accounts. This could allow an authenticated remote attacker to assign administrative groups to otherwise non-privileged user accounts.	6.6	More Details
CVE-2023-23396	Microsoft Excel Denial of Service Vulnerability	6.5	More Details
CVE-2023-27271	In SAP BusinessObjects Business Intelligence Platform (Web Services) - versions 420, 430, an attacker can control a malicious BOE server, forcing the application server to connect to its own admintools, leading to a high impact on availability.	6.5	More Details
CVE-2023-0749	The Ocean Extra WordPress plugin before 2.1.3 does not ensure that the template to be loaded via a shortcode is actually a template, allowing any authenticated users such as subscriber to retrieve the content of arbitrary posts, such as draft, private or even password protected ones.	6.5	More Details
CVE-2023-0772	The Popup Builder by OptinMonster WordPress plugin before 2.12.2 does not ensure that the campaign to be loaded via some shortcodes is actually a campaign, allowing any authenticated users such as subscriber to retrieve the content of arbitrary posts, like draft, private or even password protected ones.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22301	The kernel subsystem hmdfs within OpenHarmony-v3.1.5 and prior versions has an arbitrary memory accessing vulnerability which network attackers can launch a remote attack to obtain kernel memory data of the target system.	6.5	More Details
CVE-2023-27589	Minio is a Multi-Cloud Object Storage framework. Starting with RELEASE.2020-12-23T02-24-12Z and prior to RELEASE.2023-03-13T19-46-17Z, a user with `consoleAdmin` permissions can potentially create a user that matches the root credential `accessKey`. Once this user is created successfully, the root credential ceases to work appropriately. The issue is patched in RELEASE.2023-03-13T19-46-17Z. There are ways to work around this via adding higher privileges to the disabled root user via `mc admin policy set`.	6.5	More Details
CVE-2023-25618	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an unused class for error handling in which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information.	6.5	More Details
CVE-2023-24922	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	6.5	More Details
CVE-2023-27896	In SAP BusinessObjects Business Intelligence Platform - version 420, 430, an attacker can control a malicious BOE server, forcing the application server to connect to its own CMS, leading to a high impact on availability.	6.5	More Details
CVE-2023-24906	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	6.5	More Details
CVE-2023-24890	Microsoft OneDrive for iOS Security Feature Bypass Vulnerability	6.5	More Details
CVE-2023-0350	Akuvox E11 does not ensure that a file extension is associated with the file provided. This could allow an attacker to upload a file to the device by changing the extension of a malicious file to an accepted file type.	6.5	More Details
CVE-2023-24870	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27073	A Cross-Site Request Forgery (CSRF) in Online Food Ordering System v1.0 allows attackers to change user details and credentials via a crafted POST request.	6.5	More Details
CVE-2023-24866	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	6.5	More Details
CVE-2023-23411	Windows Hyper-V Denial of Service Vulnerability	6.5	More Details
CVE-2023-24180	Libelfin v0.3 was discovered to contain an integer overflow in the load function at elf/mmap_loader.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted elf file.	6.5	More Details
CVE-2022-43902	IBM MQ 9.2 CD, 9.2 LTS, 9.3 CD, and 9.3 LTS is vulnerable to a denial of service attack caused by specially crafted PCF or MQSC messages. IBM X-Force ID: 240832.	6.5	More Details
CVE-2023-27270	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information.	6.5	More Details
CVE-2023-1361	SQL Injection in GitHub repository unilogies/bumsys prior to v2.0.2.	6.5	More Details
CVE-2023-1201	Improper access control in the secure messages feature in Devolutions Server 2022.3.12 and below allows an authenticated attacker that possesses the message UUID to access the data it contains.	6.5	More Details
CVE-2023-1203	Improper removal of sensitive data in the entry edit feature of Hub Business submodule in Devolutions Remote Desktop Manager PowerShell Module 2022.3.1.5 and earlier allows an authenticated user to access sensitive data on entries that were edited using the affected submodule.	6.5	More Details
CVE-2023-24857	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0355	Akuvox E11 uses a hard-coded cryptographic key, which could allow an attacker to decrypt sensitive information.	6.5	More Details
CVE-2023-24863	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	6.5	More Details
CVE-2023-24865	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	6.5	More Details
CVE-2022-4289	An issue has been discovered in GitLab affecting all versions starting from 15.3 before 15.7.8, versions of 15.8 before 15.8.4, and version 15.9 before 15.9.2. Google IAP details in Prometheus integration were not hidden, could be leaked from instance, group, or project settings to other users.	6.4	More Details
CVE-2023-0978	A command injection vulnerability in Trellix Intelligent Sandbox CLI for version 5.2 and earlier, allows a local user to inject and execute arbitrary operating system commands using specially crafted strings. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI command. The vulnerability allows the attack	6.4	More Details
CVE-2023-1366	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0. It has been classified as critical. This affects the function query of the file admin/categories/manage_category.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222873 was assigned to this vulnerability.	6.3	More Details
CVE-2023-1378	A vulnerability classified as critical was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. This vulnerability affects unknown code of the file paypalsuccess.php of the component POST Parameter Handler. The manipulation of the argument cusid 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-222904.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1364	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file category.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222871.	6.3	More Details
CVE-2023-1358	A vulnerability, which was classified as critical, was found in SourceCodester Gadget Works Online Ordering System 1.0. This affects an unknown part of the file /philosophy/admin/login.php of the component POST Parameter Handler. The manipulation of the argument user_email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222861 was assigned to this vulnerability.	6.3	More Details
CVE-2023-1292	A vulnerability has been found in SourceCodester Sales Tracker Management System 1.0 and classified as critical. This vulnerability affects the function delete_client of the file classes/Master.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. VDB-222646 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-1321	A vulnerability has been found in lmxcms 1.41 and classified as critical. Affected by this vulnerability is the function update of the file AcquisiAction.class.php. The manipulation of the argument id with the input -1 and updatexml(0,concat(0x7e,user()),1)# leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222727.	6.3	More Details
CVE-2023-1351	A vulnerability classified as critical has been found in SourceCodester Computer Parts Sales and Inventory System 1.0. This affects an unknown part of the file cust_transac.php. The manipulation of the argument phonenumber leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222849 was assigned to this vulnerability.	6.3	More Details
CVE-2023-1290	A vulnerability, which was classified as critical, has been found in SourceCodester Sales Tracker Management System 1.0. Affected by this issue is some unknown functionality of the file admin/clients/view_client.php. The manipulation of the argument id leads to sql injection. 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-222644.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1300	A vulnerability classified as critical was found in SourceCodester COVID 19 Testing Management System 1.0. Affected by this vulnerability is an unknown functionality of the file patient-report.php of the component POST Parameter Handler. The manipulation of the argument searchdata leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222661 was assigned to this vulnerability.	6.3	More Details
CVE-2023-23389	Microsoft Defender Elevation of Privilege Vulnerability	6.3	More Details
CVE-2023-1308	A vulnerability classified as critical has been found in SourceCodester Online Graduate Tracer System 1.0. Affected is an unknown function of the file admin/adminlog.php. The manipulation of the argument user 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-222696.	6.3	More Details
CVE-2023-1398	A vulnerability classified as critical was found in XiaoBingBy TeaCMS 2.0. Affected by this vulnerability is an unknown functionality of the file /admin/upload. The manipulation leads to path traversal: '../filedir'. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222985 was assigned to this vulnerability.	6.3	More Details
CVE-2023-1394	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0. It has been classified as critical. This affects the function mysqli_query of the file bsitemp.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222981 was assigned to this vulnerability.	6.3	More Details
CVE-2023-1392	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. Affected by this vulnerability is the function save_menu. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222979.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1301	A vulnerability, which was classified as critical, has been found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. Affected by this issue is some unknown functionality of the file deleteorder.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-222662 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-1303	A vulnerability was found in UCMS 1.6 and classified as critical. This issue affects some unknown processing of the file sadmin/fileedit.php of the component System File Management Module. The manipulation of the argument file leads to unrestricted upload. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-222683.	6.3	More Details
CVE-2023-1322	A vulnerability was found in lmxcms 1.41 and classified as critical. Affected by this issue is the function reply of the file BookAction.class.php. The manipulation of the argument id with the input 1) and updatexml(0,concat(0x7e,user()),1)# leads to sql injection. 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-222728.	6.3	More Details
CVE-2023-0746	The help page in GigaVUE-FM, when using GigaVUE-OS software version 5.0 202, does not require an authenticated user. An attacker could enforce a user into inserting malicious JavaScript code into the URI, that could lead to a Reflected Cross site Scripting.	6.3	More Details
CVE-2023-1311	A vulnerability, which was classified as critical, was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. This affects an unknown part of the file large.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222699.	6.3	More Details
CVE-2023-1310	A vulnerability, which was classified as critical, has been found in SourceCodester Online Graduate Tracer System 1.0. Affected by this issue is some unknown functionality of the file admin/prof.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-222698 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1309	A vulnerability classified as critical was found in SourceCodester Online Graduate Tracer System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/search_it.php. The manipulation of the argument input leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222697 was assigned to this vulnerability.	6.3	More Details
CVE-2023-1350	A vulnerability was found in liferea. It has been rated as critical. Affected by this issue is the function update_job_run of the file src/update.c of the component Feed Enrichment. The manipulation of the argument source with the input ldate >/tmp/bad-item-link.txt leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 8d8b5b963fa64c7a2122d1bbfbb0bed46e813e59. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-222848.	6.3	More Details
CVE-2023-1291	A vulnerability, which was classified as critical, was found in SourceCodester Sales Tracker Management System 1.0. This affects an unknown part of the file admin/clients/manage_client.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222645 was assigned to this vulnerability.	6.3	More Details
CVE-2022-22075	Information Disclosure in Graphics during GPU context switch.	6.2	More Details
CVE-2023-25947	The bundle management subsystem within OpenHarmony-v3.1.4 and prior versions has a null pointer reference vulnerability which local attackers can exploit this vulnerability to cause a DoS attack to the system when installing a malicious HAP package.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27484	crossplane-runtime is a set of go libraries used to build Kubernetes controllers in Crossplane and its related stacks. In affected versions an already highly privileged user able to create or update Compositions can specify an arbitrarily high index in a patch's `ToFieldPath`, which could lead to excessive memory usage once such Composition is selected for a Composite resource. Compositions allow users to specify patches inserting elements into arrays at an arbitrary index. When a Composition is selected for a Composite Resource, patches are evaluated and if a specified index is greater than the current size of the target slice, Crossplane will grow that slice up to the specified index, which could lead to an excessive amount of memory usage and therefore the Pod being OOM-Killed. The index is already capped to the maximum value for a uint32 (4294967295) when parsed, but that is still an unnecessarily large value. This issue has been addressed in versions 1.11.2, 1.10.3, and 1.9.2. Users are advised to upgrade. Users unable to upgrade can restrict write privileges on Compositions to only admin users as a workaround.	6.2	More Details
CVE-2023-1320	Cross-site Scripting (XSS) - Stored in GitHub repository osticket/osticket prior to v1.16.6.	6.1	More Details
CVE-2023-0628	Docker Desktop before 4.17.0 allows an attacker to execute an arbitrary command inside a Dev Environments container during initialization by tricking a user to open a crafted malicious docker-desktop:// URL.	6.1	More Details
CVE-2023-27211	A cross-site scripting (XSS) vulnerability in /admin/navbar.php of Online Pizza Ordering System 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the page parameter.	6.1	More Details
CVE-2022-48111	A cross-site scripting (XSS) vulnerability in the check_login function of SIPE s.r.l WI400 between version 8 and 11 included allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the f parameter.	6.1	More Details
CVE-2023-24657	phpipam v1.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the closeClass parameter at /subnet-masks/popup.php.	6.1	More Details
CVE-2023-27093	Cross Site Scripting vulnerability found in My-Blog allows attackers to cause a denial of service via the Post function.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27212	A cross-site scripting (XSS) vulnerability in /php-opos/signup.php of Online Pizza Ordering System 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the redirect parameter.	6.1	More Details
CVE-2022-23790	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Firmanet Software and Technology Customer Relation Manager allows Cross-Site Scripting (XSS).This issue affects Customer Relation Manager: before 2022.03.13.	6.1	More Details
CVE-2023-27208	A cross-site scripting (XSS) vulnerability in /php-opos/login.php of Online Pizza Ordering System 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the redirect parameter.	6.1	More Details
CVE-2023-26457	SAP Content Server - version 7.53, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker can read and modify some sensitive information but cannot delete the data.	6.1	More Details
CVE-2023-1362	Improper Restriction of Rendered UI Layers or Frames in GitHub repository unilogies/bumsys prior to v2.0.2.	6.1	More Details
CVE-2021-46875	An issue was discovered in eZ Platform Ibexa Kernel before 1.3.1.1. An XSS attack can occur because JavaScript code can be uploaded in a .html or .js file.	6.1	More Details
CVE-2023-27895	SAP Authenticator for Android - version 1.3.0, allows the screen to be captured, if an authorized attacker installs a malicious app on the mobile device. The attacker could extract the currently views of the OTP and the secret OTP alphanumeric token during the token setup. On successful exploitation, an attacker can read some sensitive information but cannot modify and delete the data.	6.1	More Details
CVE-2022-23791	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Firmanet Software and Technology Customer Relation Manager allows Cross-Site Scripting (XSS).This issue affects Customer Relation Manager: before 2022.03.13.	6.1	More Details
CVE-2023-27206	A cross-site scripting (XSS) vulnerability in /kruxton/navbar.php of Best POS Management System 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the page parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4195	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Firmanet Software and Technology Customer Relation Manager allows XSS Targeting HTML Attributes.This issue affects Customer Relation Manager: before 2022.03.13.	6.1	More Details
CVE-2023-24279	A cross-site scripting (XSS) vulnerability in Open Networking Foundation ONOS from version v1.9.0 to v2.7.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the url parameter of the API documentation dashboard.	6.1	More Details
CVE-2023-0021	Due to insufficient encoding of user input, SAP NetWeaver - versions 700, 701, 702, 731, 740, 750, allows an unauthenticated attacker to inject code that may expose sensitive data like user ID and password, which could lead to reflected Cross-Site scripting. These endpoints are normally exposed over the network and successful exploitation can partially impact confidentiality of the application.	6.1	More Details
CVE-2023-27483	crossplane-runtime is a set of go libraries used to build Kubernetes controllers in Crossplane and its related stacks. An out of memory panic vulnerability has been discovered in affected versions. Applications that use the `Paved` type's `SetValue` method with user provided input without proper validation might use excessive amounts of memory and cause an out of memory panic. In the fieldpath package, the Paved.SetValue method sets a value on the Paved object according to the provided path, without any validation. This allows setting values in slices at any provided index, which grows the target array up to the requested index, the index is currently capped at max uint32 (4294967295) given how indexes are parsed, but that is still an unnecessarily large value. If callers are not validating paths' indexes on their own, which most probably are not going to do, given that the input is parsed directly in the SetValue method, this could allow users to consume arbitrary amounts of memory. Applications that do not use the `Paved` type's `SetValue` method are not affected. This issue has been addressed in versions 0.16.1 and 0.19.2. Users are advised to upgrade. Users unable to upgrade can parse and validate the path before passing it to the `SetValue` method of the `Paved` type, constraining the index size as deemed appropriate.	5.9	More Details
CVE-2022-33260	Memory corruption due to stack based buffer overflow in core while sending command from USB of large size.	5.9	More Details
CVE-2022-47171	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Paul C. Schroeder IP Vault – WP Firewall plugin <= 1.1 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4331	An issue has been discovered in GitLab EE affecting all versions starting from 15.1 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. If a group with SAML SSO enabled is transferred to a new namespace as a child group, it's possible previously removed malicious maintainer or owner of the child group can still gain access to the group via SSO or a SCIM token to perform actions on the group.	5.7	More Details
CVE-2023-1352	A vulnerability, which was classified as critical, has been found in SourceCodester Design and Implementation of Covid-19 Directory on Vaccination System 1.0. This issue affects some unknown processing of the file /admin/login.php. The manipulation of the argument txtusername/txtpassword leads to sql injection. The attack may be initiated remotely. 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. The associated identifier of this vulnerability is VDB-222851.	5.6	More Details
CVE-2023-24923	Microsoft OneDrive for Android Information Disclosure Vulnerability	5.5	More Details
CVE-2023-23391	Office for Android Spoofing Vulnerability	5.5	More Details
CVE-2023-24882	Microsoft OneDrive for Android Information Disclosure Vulnerability	5.5	More Details
CVE-2023-24862	Windows Secure Channel Denial of Service Vulnerability	5.5	More Details
CVE-2023-0483	An issue has been discovered in GitLab affecting all versions starting from 12.1 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. It was possible for a project maintainer to extract a Datadog integration API key by modifying the site.	5.5	More Details
CVE-2023-23409	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability	5.5	More Details
CVE-2023-23394	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27119	WebAssembly v1.0.29 was discovered to contain a segmentation fault via the component wabt::Decompiler::WrapChild.	5.5	More Details
CVE-2022-47480	In telephony service, there is a missing permission check. This could lead to local denial of service in telephone service with no additional execution privileges needed.	5.5	More Details
CVE-2022-47474	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2022-47456	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-2023-24577	McAfee Total Protection prior to 16.0.50 allows attackers to elevate user privileges due to Improper Link Resolution via registry keys. This could enable a user with lower privileges to execute unauthorized tasks.	5.5	More Details
CVE-2022-47457	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-2022-47458	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-2022-47459	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-2022-47460	In gpu device, there is a memory corruption due to a use after free. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-47471	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2022-47472	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47473	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2022-47475	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2022-47454	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-2022-47476	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2022-47477	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2022-47478	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2022-47479	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	5.5	More Details
CVE-2023-1355	NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.1402.	5.5	More Details
CVE-2022-47481	In telephony service, there is a missing permission check. This could lead to local denial of service in telephone service with no additional execution privileges needed.	5.5	More Details
CVE-2022-47482	In telephony service, there is a missing permission check. This could lead to local denial of service in telephone service with no additional execution privileges needed.	5.5	More Details
CVE-2022-47483	In telephony service, there is a missing permission check. This could lead to local denial of service in telephone service with no additional execution privileges needed.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47484	In telephony service, there is a missing permission check. This could lead to local denial of service in telephone service with no additional execution privileges needed.	5.5	More Details
CVE-2022-47455	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-2023-24578	McAfee Total Protection prior to 16.0.49 allows attackers to elevate user privileges due to DLL sideloading. This could enable a user with lower privileges to execute unauthorized tasks.	5.5	More Details
CVE-2022-47453	In wcn service, there is a possible missing params check. This could lead to local denial of service in wcn service.	5.5	More Details
CVE-2023-24465	Communication Wi-Fi subsystem within OpenHarmony-v3.1.4 and prior versions, OpenHarmony-v3.0.7 and prior versions has a null pointer reference vulnerability which local attackers can exploit this vulnerability to cause the current application to crash.	5.5	More Details
CVE-2023-27114	radare2 v5.8.3 was discovered to contain a segmentation fault via the component wasm_dis at p/wasm/wasm.c.	5.5	More Details
CVE-2023-27115	WebAssembly v1.0.29 was discovered to contain a segmentation fault via the component wabt::cat_compute_size.	5.5	More Details
CVE-2023-27116	WebAssembly v1.0.29 discovered to contain an abort in CWriter::MangleType.	5.5	More Details
CVE-2023-24579	McAfee Total Protection prior to 16.0.51 allows attackers to trick a victim into uninstalling the application via the command prompt.	5.5	More Details
CVE-2023-24920	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	5.4	More Details
CVE-2022-47141	Cross-Site Request Forgery (CSRF) vulnerability in Seerox WP Dynamic Keywords Injector plugin <= 2.3.15 versions.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47147	Cross-Site Request Forgery (CSRF) vulnerability in Kesz1 Technologies ipBlockList plugin <= 1.0 versions.	5.4	More Details
CVE-2023-1315	Cross-site Scripting (XSS) - Reflected in GitHub repository osticket/osticket prior to v1.16.6.	5.4	More Details
CVE-2023-26950	onekeyadmin v1.3.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Title parameter under the Adding Categories module.	5.4	More Details
CVE-2023-1316	Cross-site Scripting (XSS) - Stored in GitHub repository osticket/osticket prior to v1.16.6.	5.4	More Details
CVE-2023-0066	The Companion Sitemap Generator WordPress plugin through 4.5.1.1 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-2023-1317	Cross-site Scripting (XSS) - Reflected in GitHub repository osticket/osticket prior to v1.16.6.	5.4	More Details
CVE-2023-24921	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	5.4	More Details
CVE-2023-1270	Cross-site Scripting in GitHub repository btcpayserver/btcpayserver prior to 1.8.3.	5.4	More Details
CVE-2023-24919	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	5.4	More Details
CVE-2022-3758	An issue has been discovered in GitLab affecting all versions starting from 15.5 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. Due to improper permissions checks an unauthorised user was able to read, add or edit a users private snippet.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27069	A stored cross-site scripting (XSS) vulnerability in TotalJS OpenPlatform commit b80b09d allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the account name field.	5.4	More Details
CVE-2023-27070	A stored cross-site scripting (XSS) vulnerability in TotalJS OpenPlatform commit b80b09d allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the platform name field.	5.4	More Details
CVE-2023-26952	onekeyadmin v1.3.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Add Menu module.	5.4	More Details
CVE-2023-1318	Cross-site Scripting (XSS) - Generic in GitHub repository osticket/osticket prior to v1.16.6.	5.4	More Details
CVE-2023-24891	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	5.4	More Details
CVE-2023-24879	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	5.4	More Details
CVE-2023-24282	An arbitrary file upload vulnerability in Poly Trio 8800 7.2.2.1094 allows attackers to execute arbitrary code via a crafted ringtone file.	5.4	More Details
CVE-2022-4007	A issue has been discovered in GitLab CE/EE affecting all versions from 15.3 prior to 15.7.8, version 15.8 prior to 15.8.4, and version 15.9 prior to 15.9.2 A cross-site scripting vulnerability was found in the title field of work items that allowed attackers to perform arbitrary actions on behalf of victims at client side.	5.4	More Details
CVE-2023-23326	A Stored Cross-Site Scripting (XSS) vulnerability exists in AvantFAX 3.3.7. An authenticated low privilege user can inject arbitrary Javascript into their e-mail address which is executed when an administrator logs into AvantFAX to view the admin dashboard. This may result in stealing an administrator's session cookie and hijacking their session.	5.4	More Details
CVE-2023-24975	IBM Spectrum Symphony 7.3 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: 247030.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4661	The Widgets for WooCommerce Products on Elementor WordPress plugin before 1.0.8 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-2022-4652	The Video Background WordPress plugin before 2.7.5 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-2023-25991	Cross-Site Request Forgery (CSRF) vulnerability in RegistrationMagic plugin <= 5.1.9.2 versions.	5.4	More Details
CVE-2023-0073	The Client Logo Carousel WordPress plugin through 3.0.0 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-2023-0172	The Juicer WordPress plugin before 1.11 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-2023-0219	The FluentSMTP WordPress plugin before 2.2.3 does not sanitize or escape email content, making it vulnerable to stored cross-site scripting attacks (XSS) when an administrator views the email logs. This exploit requires other plugins to enable users to send emails with unfiltered HTML.	5.4	More Details
CVE-2022-4466	The WordPress Infinite Scroll WordPress plugin before 5.6.0.3 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-2023-0538	The Campaign URL Builder WordPress plugin before 1.8.2 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 Number	Description	Base Score	Reference
CVE-2023-25973	Cross-Site Request Forgery (CSRF) vulnerability in Lucian Apostol Auto Affiliate Links plugin <= 6.3.0.2 versions.	5.4	More Details
CVE-2021-46876	An issue was discovered in eZ Publish Ibexa Kernel before 7.5.15.1. The /user/sessions endpoint can be abused to determine account existence.	5.3	More Details
CVE-2023-27268	SAP NetWeaver AS Java (Object Analyzing Service) - version 7.50, does not perform necessary authorization checks, allowing an unauthenticated attacker to attach to an open interface and make use of an open naming and directory API to access a service which will enable them to access but not modify server settings and data with no effect on availability., resulting in escalation of privileges.	5.3	More Details
CVE-2023-24526	SAP NetWeaver Application Server Java for Classload Service - version 7.50, does not perform any authentication checks for functionalities that require user identity, resulting in escalation of privileges. This failure has a low impact on confidentiality of the data such that an unassigned user can read non-sensitive server data.	5.3	More Details
CVE-2023-24532	The ScalarMult and ScalarBaseMult methods of the P256 Curve may return an incorrect result if called with some specific unreduced scalars (a scalar larger than the order of the curve). This does not impact usages of crypto/ecdsa or crypto/ecdh.	5.3	More Details
CVE-2023-26460	Cache Management Service in SAP NetWeaver Application Server for Java - version 7.50, does not perform any authentication checks for functionalities that require user identity	5.3	More Details
CVE-2023-27904	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier prints an error stack trace on agent-related pages when agent connections are broken, potentially revealing information about Jenkins configuration that is otherwise inaccessible to attackers.	5.3	More Details
CVE-2023-0223	An issue has been discovered in GitLab affecting all versions starting from 15.5 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. Non-project members could retrieve release descriptions via the API, even if the release visibility is restricted to project members only in the project settings.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25170	PrestaShop is an open source e-commerce web application that, prior to version 8.0.1, is vulnerable to cross-site request forgery (CSRF). When authenticating users, PrestaShop preserves session attributes. Because this does not clear CSRF tokens upon login, this might enable same-site attackers to bypass the CSRF protection mechanism by performing an attack similar to a session-fixation. The problem is fixed in version 8.0.1.	5.0	More Details
CVE-2022-4315	An issue has been discovered in GitLab DAST analyzer affecting all versions starting from 2.0 before 3.0.55, which sends custom request headers with every request on the authentication page.	5.0	More Details
CVE-2023-27894	SAP BusinessObjects Business Intelligence Platform (Web Services) - versions 420, 430, allows an attacker to inject arbitrary values as CMS parameters to perform lookups on the internal network which is otherwise not accessible externally. On successful exploitation, attacker can scan internal network to determine internal infrastructure for further attacks like remote file inclusion, retrieve server files, bypass firewall and force the vulnerable server to execute malicious requests, resulting in sensitive information disclosure. This causes limited impact on confidentiality of data.	5.0	More Details
CVE-2023-1369	A vulnerability was found in TG Soft Vir.IT eXplorer 9.4.86.0. It has been rated as problematic. This issue affects the function 0x82730088 in the library VIRAGTLT.sys of the component IoControlCode Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 9.5 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-222875.	5.0	More Details
CVE-2023-27309	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.2). The client query handler of the affected application fails to check for proper permissions for specific write queries. This could allow an authenticated remote attacker to perform unauthorized actions.	5.0	More Details
CVE-2023-1293	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0 and classified as critical. This issue affects the function mysqli_query of the file admin_cs.php. The manipulation leads to sql injection. The attack may be initiated remotely. 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. The associated identifier of this vulnerability is VDB-222647.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23638	A deserialization vulnerability existed when dubbo generic invoke, which could lead to malicious code execution. This issue affects Apache Dubbo 2.7.x version 2.7.21 and prior versions; Apache Dubbo 3.0.x version 3.0.13 and prior versions; Apache Dubbo 3.1.x version 3.1.5 and prior versions.	5.0	More Details
CVE-2022-4462	An issue has been discovered in GitLab affecting all versions starting from 12.8 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. This vulnerability could allow a user to unmask the Discord Webhook URL through viewing the raw API response.	5.0	More Details
CVE-2022-4317	An issue has been discovered in GitLab DAST analyzer affecting all versions starting from 1.47 before 3.0.51, which sends custom request headers in redirects.	5.0	More Details
CVE-2023-0845	Consul and Consul Enterprise allowed an authenticated user with service:write permissions to trigger a workflow that causes Consul server and client agents to crash under certain circumstances. This vulnerability was fixed in Consul 1.14.5.	4.9	More Details
CVE-2023-0888	An improper neutralization of directives in dynamically evaluated code vulnerability in the WiFi Battery embedded web server in versions L90/U70 and L92/U92 can be used to gain administrative access to the WiFi communication module. An authenticated user, having access to both the medical device WiFi network (such as a biomedical engineering staff member) and the specific B.Braun Battery Pack SP with WiFi web server credentials, could get administrative (root) access on the infusion pump communication module. This could be used as a vector to start further attacks	4.9	More Details
CVE-2023-23760	A path traversal vulnerability was identified in GitHub Enterprise Server that allowed remote code execution when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to versions 3.8 and was fixed in versions 3.7.7, 3.6.10, 3.5.14, and 3.4.17. This vulnerability was reported via the GitHub Bug Bounty program.	4.9	More Details
CVE-2023-23327	An Information Disclosure vulnerability exists in AvantFAX 3.3.7. Backups of the AvantFAX sent/received faxes, and database backups are stored using the current date as the filename and hosted on the web server without access controls.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47595	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WP Go Maps (formerly WP Google Maps) plugin <= 9.0.15 versions.	4.9	More Details
CVE-2023-1286	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.19.	4.8	More Details
CVE-2023-27164	An arbitrary file upload vulnerability in Halo up to v1.6.1 allows attackers to execute arbitrary code via a crafted .md file.	4.8	More Details
CVE-2023-1319	Cross-site Scripting (XSS) - Stored in GitHub repository osticket/osticket prior to v1.16.6.	4.8	More Details
CVE-2023-0844	The Namaste! LMS WordPress plugin before 2.6 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2016-15028	A vulnerability was found in ICEPAY REST-API-NET 0.9. It has been declared as problematic. Affected by this vulnerability is the function RestClient of the file Classes/RestClient.cs of the component Checksum Validation. The manipulation leads to improper validation of integrity check value. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. Upgrading to version 1.0 is able to address this issue. The patch is named 61f6b8758e5c971abff5f901cfa9f231052b775f. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-222847.	4.8	More Details
CVE-2023-1312	Cross-site Scripting (XSS) - Reflected in GitHub repository pimcore/pimcore prior to 10.5.19.	4.8	More Details
CVE-2023-1276	A vulnerability, which was classified as critical, has been found in SUL1SS_shop. This issue affects some unknown processing of the file application\merch\controller\Order.php. The manipulation of the argument keyword leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-222599.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1391	A vulnerability, which was classified as problematic, was found in SourceCodester Online Tours & Travels Management System 1.0. Affected is an unknown function of the file admin/ab.php. The manipulation of the argument img leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-222978 is the identifier assigned to this vulnerability.	4.7	More Details
CVE-2023-1328	A vulnerability was found in Guizhou 115cms 4.2. It has been classified as problematic. Affected is an unknown function of the file /admin/content/index. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-222738 is the identifier assigned to this vulnerability.	4.7	More Details
CVE-2023-1360	A vulnerability was found in SourceCodester Employee Payslip Generator with Sending Mail 1.2.0 and classified as critical. This issue affects some unknown processing of the file classes/Users.php?f=save of the component New User Creation. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222863.	4.7	More Details
CVE-2023-20064	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device.	4.6	More Details
CVE-2022-46752	Dell BIOS contains an Improper Authorization vulnerability. An unauthenticated physical attacker may potentially exploit this vulnerability, leading to denial of service.	4.6	More Details
CVE-2023-23408	Azure Apache Ambari Spoofing Vulnerability	4.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27903	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier creates a temporary file in the default temporary directory with the default permissions for newly created files when uploading a file parameter through the CLI, potentially allowing attackers with access to the Jenkins controller file system to read and write the file before it is used.	4.4	More Details
CVE-2023-0193	NVIDIA CUDA Toolkit SDK contains a vulnerability in cuobjdump, where a local user running the tool against a malicious binary may cause an out-of-bounds read, which may result in a limited denial of service and limited information disclosure.	4.4	More Details
CVE-2023-24999	HashiCorp Vault and Vault Enterprise’s approle auth method allowed any authenticated user with access to an approle destroy endpoint to destroy the secret ID of any other role by providing the secret ID accessor. This vulnerability is fixed in Vault 1.13.0, 1.12.4, 1.11.8, 1.10.11 and above.	4.4	More Details
CVE-2023-1374	The Solidres plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'currency_name' parameter in versions up to, and including, 0.9.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with administrator privileges to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details
CVE-2023-24880	Windows SmartScreen Security Feature Bypass Vulnerability	4.4	More Details
CVE-2023-1335	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the ucss_connect function in versions up to, and including, 1.7.1. This makes it possible for authenticated attackers with subscriber-level access to connect a new license key to the site.	4.3	More Details
CVE-2023-1345	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the queue_posts function. This makes it possible for unauthenticated attackers to modify the plugin's cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-1336	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized settings update due to a missing capability check on the ajax_deactivate function in versions up to, and including, 1.7.1. This makes it possible for authenticated attackers with subscriber-level access to disable caching.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1072	An issue has been discovered in GitLab affecting all versions starting from 9.0 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. It was possible to trigger a resource depletion attack due to improper filtering for number of requests to read commits details.	4.3	More Details
CVE-2023-1337	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized data loss due to a missing capability check on the clear_uucss_logs function in versions up to, and including, 1.7.1. This makes it possible for authenticated attackers with subscriber-level access to delete plugin log files.	4.3	More Details
CVE-2023-1341	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the ajax_deactivate function. This makes it possible for unauthenticated attackers to turn off caching via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-1338	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized cache modification due to a missing capability check on the attach_rule function in versions up to, and including, 1.7.1. This makes it possible for authenticated attackers with subscriber-level access to modify cache rules.	4.3	More Details
CVE-2022-47422	Cross-Site Request Forgery (CSRF) vulnerability in HM Plugin Accept Stripe Donation – AidWP plugin <= 3.1.5 versions.	4.3	More Details
CVE-2023-1339	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized settings update due to a missing capability check on the uucss_update_rule function in versions up to, and including, 1.7.1. This makes it possible for authenticated attackers with subscriber-level access to update caching rules.	4.3	More Details
CVE-2014-125093	A vulnerability has been found in Ad Blocking Detector Plugin up to 1.2.1 on WordPress and classified as problematic. This vulnerability affects unknown code of the file ad-blocking-detector.php. The manipulation leads to information disclosure. The attack can be initiated remotely. Upgrading to version 1.2.2 is able to address this issue. The patch is identified as 3312b9cd79e5710d1e282fc9216a4e5ab31b3d94. It is recommended to upgrade the affected component. VDB-222610 is the identifier assigned to this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1342	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the ucss_connect function. This makes it possible for unauthenticated attackers to connect the site to a new license key via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-1340	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the clear_uucss_logs function. This makes it possible for unauthenticated attackers to clear plugin logs via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2020-5002	IBM Financial Transaction Manager 3.2.0 through 3.2.10 could allow an authenticated user to perform unauthorized actions due to improper validation. IBM X-Force ID: 192954.	4.3	More Details
CVE-2023-1346	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the clear_page_cache function. This makes it possible for unauthenticated attackers to clear the plugin's cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-1334	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized cache modification due to a missing capability check on the queue_posts function in versions up to, and including, 1.7.1. This makes it possible for authenticated attackers with subscriber-level access to modify the plugin's cache.	4.3	More Details
CVE-2022-47166	Cross-Site Request Forgery (CSRF) vulnerability in voidCoders Void Contact Form 7 Widget For Elementor Page Builder plugin <= 2.1.1 versions.	4.3	More Details
CVE-2023-1333	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the clear_page_cache function in versions up to, and including, 1.7.1. This makes it possible for authenticated attackers with subscriber-level access to delete the plugin's cache.	4.3	More Details
CVE-2022-47143	Cross-Site Request Forgery (CSRF) vulnerability in Themeisle Multiple Page Generator Plugin – MPG plugin <= 3.3.9 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47155	Cross-Site Request Forgery (CSRF) vulnerability in Supsystic Slider by Supsystic plugin <= 1.8.5 versions.	4.3	More Details
CVE-2022-47162	Cross-Site Request Forgery (CSRF) vulnerability in Dannie Herdyawan DH – Anti AdBlocker plugin <= 36 versions.	4.3	More Details
CVE-2022-47154	Cross-Site Request Forgery (CSRF) vulnerability in Pi Websolution CSS JS Manager, Async JavaScript, Defer Render Blocking CSS supports WooCommerce plugin <= 2.4.49 versions.	4.3	More Details
CVE-2023-27902	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier shows temporary directories related to job workspaces, which allows attackers with Item/Workspace permission to access their contents.	4.3	More Details
CVE-2023-23711	Cross-Site Request Forgery (CSRF) vulnerability in A2 Hosting A2 Optimized WP plugin <= 3.0.4 versions.	4.3	More Details
CVE-2023-24911	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	4.3	More Details
CVE-2023-22700	Cross-Site Request Forgery (CSRF) vulnerability in PixelYourSite PixelYourSite – Your smart PIXEL (TAG) Manager plugin <= 9.3.0 versions.	4.3	More Details
CVE-2022-2258	In affected versions of Octopus Deploy it is possible for a user to view Tagsets without being explicitly assigned permissions to view these items	4.3	More Details
CVE-2022-2259	In affected versions of Octopus Deploy it is possible for a user to view Workerpools without being explicitly assigned permissions to view these items	4.3	More Details
CVE-2022-3381	An issue has been discovered in GitLab affecting all versions starting from 10.0 to 15.7.8, 15.8 prior to 15.8.4 and 15.9 prior to 15.9.2. A crafted URL could be used to redirect users to arbitrary sites	4.3	More Details
CVE-2022-47443	Cross-Site Request Forgery (CSRF) vulnerability in Daniel Powney Multi Rating plugin <= 5.0.5 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1344	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the uucss_update_rule function. This makes it possible for unauthenticated attackers to modify the plugin's cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2022-47440	Cross-Site Request Forgery (CSRF) vulnerability in Joseph C Dolson My Tickets plugin <= 1.9.10 versions.	4.3	More Details
CVE-2023-1343	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the attach_rule function. This makes it possible for unauthenticated attackers to modify the plugin's cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-0083	The ArKUI framework subsystem within OpenHarmony-v3.1.5 and prior versions, OpenHarmony-v3.0.7 and prior versions has an Improper Input Validation vulnerability which local attackers can exploit this vulnerability to send malicious data, causing the current application to crash.	4.0	More Details
CVE-2023-1367	Code Injection in GitHub repository alextselegidis/easyappointments prior to 1.5.0.	3.8	More Details
CVE-2023-26209	A improper restriction of excessive authentication attempts vulnerability [CWE-307] in Fortinet FortiDeceptor 3.1.x and before allows a remote unauthenticated attacker to partially exhaust CPU and memory via sending numerous HTTP requests to the login form.	3.7	More Details
CVE-2023-26208	A improper restriction of excessive authentication attempts vulnerability [CWE-307] in Fortinet FortiAuthenticator 6.4.x and before allows a remote unauthenticated attacker to partially exhaust CPU and memory via sending numerous HTTP requests to the login form.	3.7	More Details
CVE-2022-48366	An issue was discovered in eZ Platform Ibexa Kernel before 1.3.19. It allows determining account existence via a timing attack.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29056	A improper restriction of excessive authentication attempts vulnerability [CWE-307] in Fortinet FortiMail version 6.4.0, version 6.2.0 through 6.2.4 and before 6.0.9 allows a remote unauthenticated attacker to partially exhaust CPU and memory via sending numerous HTTP requests to the login form.	3.7	More Details
CVE-2023-1353	A vulnerability, which was classified as problematic, was found in SourceCodester Design and Implementation of Covid-19 Directory on Vaccination System 1.0. Affected is an unknown function of the file verification.php. The manipulation of the argument txtvaccinationID leads to cross site scripting. 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-222852.	3.5	More Details
CVE-2023-1395	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0. It has been declared as problematic. This vulnerability affects the function query of the file admin/user/list.php. The manipulation of the argument name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-222982 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-1278	A vulnerability, which was classified as problematic, has been found in IBOS up to 4.5.5. Affected by this issue is some unknown functionality of the file mobil/index.php. The manipulation of the argument accesstoken leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-222608.	3.5	More Details
CVE-2023-1349	A vulnerability, which was classified as problematic, has been found in Hsycms 3.1. Affected by this issue is some unknown functionality of the file controller\cate.php of the component Add Category Module. The manipulation of the argument title leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-222842 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-1275	A vulnerability classified as problematic was found in SourceCodester Phone Shop Sales Managements System 1.0. This vulnerability affects unknown code of the file /osms/assets/plugins/jquery-validation-1.11.1/demo/captcha/index.php of the component CAPTCHA Handler. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-222598 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1397	A vulnerability classified as problematic has been found in SourceCodester Online Student Management System 1.0. Affected is an unknown function of the file profile.php. The manipulation of the argument adminname leads to cross site scripting. 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-222984.	3.5	More Details
CVE-2023-1396	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file admin/traveller_details.php. The manipulation of the argument address leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222983.	3.5	More Details
CVE-2023-1302	A vulnerability, which was classified as problematic, was found in SourceCodester File Tracker Manager System 1.0. This affects an unknown part of the file normal/borrow1.php. The manipulation of the argument id with the input 1"><script>alert(1111)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222663.	3.5	More Details
CVE-2023-1354	A vulnerability has been found in SourceCodester Design and Implementation of Covid-19 Directory on Vaccination System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file register.php. The manipulation of the argument txtfullname/txtage/txtaddress/txtphone leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222853 was assigned to this vulnerability.	3.5	More Details
CVE-2013-10021	A vulnerability was found in dd32 Debug Bar Plugin up to 0.8 on WordPress. It has been declared as problematic. Affected by this vulnerability is the function render of the file panels/class-debug-bar-queries.php. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 0.8.1 is able to address this issue. The patch is named 0842af8f8a556bc3e39b9ef758173b0a8a9ccbfc. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-222739.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-10020	A vulnerability, which was classified as problematic, was found in MMDeveloper A Forms Plugin up to 1.4.2 on WordPress. This affects an unknown part of the file a-forms.php. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 1.4.3 is able to address this issue. The identifier of the patch is 3e693197bd69b7173cc16d8d2e0a7d501a2a0b06. It is recommended to upgrade the affected component. The identifier VDB-222609 was assigned to this vulnerability.	3.5	More Details
CVE-2017-20182	A vulnerability was found in Mobile Vikings Django AJAX Utilities up to 1.2.1 and classified as problematic. This issue affects the function Pagination of the file django_ajax/static/ajax-utilities/js/pagination.js of the component Backslash Handler. The manipulation of the argument url leads to cross site scripting. The attack may be initiated remotely. The patch is named 329eb1dd1580ca1f9d4f95bc69939833226515c9. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-222611.	3.5	More Details
CVE-2023-1363	A vulnerability, which was classified as problematic, was found in SourceCodester Computer Parts Sales and Inventory System 1.0. Affected is an unknown function of the component Add User Account. The manipulation of the argument username leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-222870 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-27477	wasmtime is a fast and secure runtime for WebAssembly. Wasmtime's code generation backend, Cranelift, has a bug on x86_64 platforms for the WebAssembly `i8x16.select` instruction which will produce the wrong results when the same operand is provided to the instruction and some of the selected indices are greater than 16. There is an off-by-one error in the calculation of the mask to the `pshufb` instruction which causes incorrect results to be returned if lanes are selected from the second vector. This codegen bug has been fixed in Wasmtiem 6.0.1, 5.0.1, and 4.0.1. Users are recommended to upgrade to these updated versions. If upgrading is not an option for you at this time, you can avoid this miscompilation by disabling the Wasm simd proposal. Additionally the bug is only present on x86_64 hosts. Other platforms such as AArch64 and s390x are not affected.	3.1	More Details
CVE-2022-47163	Cross-Site Request Forgery (CSRF) vulnerability in Tips and Tricks HQ, josh401 WP CSV to Database – Insert CSV file content into WordPress plugin <= 2.6 versions.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23395	Microsoft SharePoint Server Spoofing Vulnerability	3.1	More Details
CVE-2023-27462	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.3). The client query handler of the affected application fails to check for proper permissions for specific read queries. This could allow authenticated remote attackers to access data they are not authorized for.	3.1	More Details
CVE-2023-1296	HashiCorp Nomad and Nomad Enterprise 1.4.0 up to 1.5.0 did not correctly enforce deny policies applied to a workload's variables. Fixed in 1.4.6 and 1.5.1.	2.7	More Details
CVE-2023-1084	An issue has been discovered in GitLab CE/EE affecting all versions before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. A malicious project Maintainer may create a Project Access Token with Owner level privileges using a crafted request.	2.7	More Details
CVE-2023-1359	A vulnerability has been found in SourceCodester Gadget Works Online Ordering System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /philosophy/admin/user/controller.php?action=add of the component Add New User. The manipulation of the argument U_NAME leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-222862 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2022-37939	A potential security vulnerability has been identified in HPE Superdome Flex and Superdome Flex 280 servers. The vulnerability could be locally exploited to allow disclosure of information. HPE has made the following software to resolve the vulnerability in HPE Superdome Flex Servers v3.65.8 and Superdome Flex 280 Servers v1.45.8.	2.3	More Details
CVE-2023-0973	STEPTools v18SP1 ifcmesh library (v18.1) is affected due to a null pointer dereference, which could allow an attacker to deny application usage when reading a specially constructed file, resulting in an application crash.	2.2	More Details
CVE-2022-37950	Rejected reason: Not used in 2022	N/A	More Details
CVE-2022-37946	Rejected reason: Not used in 2022	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3678	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2022-3680	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-1015	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2022-46743	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-2022-37947	Rejected reason: Not used in 2022	N/A	More Details
CVE-2022-30996	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-2022-43399	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-2022-37951	Rejected reason: Not used in 2022	N/A	More Details
CVE-2022-37948	Rejected reason: Not used in 2022	N/A	More Details
CVE-2022-37944	Rejected reason: Not used in 2022	N/A	More Details
CVE-2023-24368	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-37943	Rejected reason: Not used in 2022	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37942	Rejected reason: Not used in 2022	N/A	More Details
CVE-2023-1173	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-2022-37949	Rejected reason: Not used in 2022	N/A	More Details
CVE-2022-37941	Rejected reason: Not used in 2022	N/A	More Details
CVE-2022-37945	Rejected reason: Not used in 2022	N/A	More Details