SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 10 January 2024

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-2023-51438	A vulnerability has been identified in SIMATIC IPC1047E (All versions with maxView Storage Manager < V4.14.00.26068 on Windows), SIMATIC IPC647E (All versions with maxView Storage Manager < V4.14.00.26068 on Windows), SIMATIC IPC847E (All versions with maxView Storage Manager < V4.14.00.26068 on Windows). In default installations of maxView Storage Manager where Redfish® server is configured for remote system management, a vulnerability has been identified that can provide unauthorized access.	10.0	More Details
CVE-2022-46839	Unrestricted Upload of File with Dangerous Type vulnerability in JS Help Desk JS Help Desk – Best Help Desk & Support Plugin.This issue affects JS Help Desk – Best Help Desk & Support Plugin: from n/a through 2.7.1.	10.0	More Details
CVE-2024-22216	In default installations of Microchip maxView Storage Manager (for Adaptec Smart Storage Controllers) where Redfish server is configured for remote system management, unauthorized access can occur, with data modification and information disclosure. This affects 3.00.23484 through 4.14.00.26064 (except for the patched versions 3.07.23980 and 4.07.00.25339).	10.0	More Details
CVE-2024-21650	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki is vulnerable to a remote code execution (RCE) attack through its user registration feature. This issue allows an attacker to execute arbitrary code by crafting malicious payloads in the "first name" or "last name" fields during user registration. This impacts all installations that have user registration enabled for guests. This vulnerability has been patched in XWiki 14.10.17, 15.5.3 and 15.8 RC1.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52218	Deserialization of Untrusted Data vulnerability in Anton Bond Woocommerce Tranzila Payment Gateway.This issue affects Woocommerce Tranzila Payment Gateway: from n/a through 1.0.8.	10.0	More Details
CVE-2023-52225	Deserialization of Untrusted Data vulnerability in Tagbox Tagbox – UGC Galleries, Social Media Widgets, User Reviews & Analytics.This issue affects Tagbox – UGC Galleries, Social Media Widgets, User Reviews & Analytics: from n/a through 3.1.	10.0	More Details
CVE-2024-21663	Discord-Recon is a Discord bot created to automate bug bounty recon, automated scans and information gathering via a discord server. Discord-Recon is vulnerable to remote code execution. An attacker is able to execute shell commands in the server without having an admin role. This vulnerability has been fixed in version 0.0.8.	9.9	More Details
CVE-2023-52219	Deserialization of Untrusted Data vulnerability in Gecka Gecka Terms Thumbnails.This issue affects Gecka Terms Thumbnails: from n/a through 1.1.	9.9	More Details
CVE-2018-25095	The Duplicator WordPress plugin before 1.3.0 does not properly escape values when its installer script replaces values in WordPress configuration files. If this installer script is left on the site after use, it could be use to run arbitrary code on the server.	9.8	More Details
CVE-2020-13878	IrfanView B3D PlugIns before version 4.56 has a B3d.dll!+27ef heap-based out-of-bounds write.	9.8	More Details
CVE-2020-13879	IrfanView B3D PlugIns before version 4.56 has a B3d.dll!+214f heap-based out-of-bounds write.	9.8	More Details
CVE-2020-13880	IrfanView B3D PlugIns before version 4.56 has a B3d.dll!+1cbf heap-based out-of-bounds write.	9.8	More Details
CVE-2023-50921	An issue was discovered on GL.iNet devices through 4.5.0. Attackers can invoke the add_user interface in the system module to gain root privileges. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7.	9.8	More Details
CVE-2023-46953	SQL Injection vulnerability in ABO.CMS v.5.9.3, allows remote attackers to execute arbitrary code via the d parameter in the Documents module.	9.8	More Details
CVE-2023-6921	Blind SQL Injection vulnerability in PrestaShow Google Integrator (PrestaShop addon) allows for data extraction and modification. This attack is possible via command insertion in one of the cookies.	9.8	More Details
CVE-2024-0321	Stack-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.3-DEV.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46308	In Plotly plotly.js before 2.25.2, plot API calls have a risk of __proto__ being polluted in expandObjectPaths or nestedProperty.	9.8	More Details
CVE-2024-22088	Lotos WebServer through 0.1.1 (commit 3eb36cc) has a use-after-free in buffer_avail() at buffer.h via a long URI, because realloc is mishandled.	9.8	More Details
CVE-2023-50643	An issue in Evernote Evernote for MacOS v.10.68.2 allows a remote attacker to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments components.	9.8	More Details
CVE-2024-21646	Azure uAMQP is a general purpose C library for AMQP 1.0. The UAMQP library is used by several clients to implement AMQP protocol communication. When clients using this library receive a crafted binary type data, an integer overflow or wraparound or memory safety issue can occur and may cause remote code execution. This vulnerability has been patched in release 2024-01-01.	9.8	More Details
CVE-2023-26999	An issue found in NetScout nGeniusOne v.6.3.4 allows a remote attacker to execute arbitrary code and cause a denial of service via a crafted file.	9.8	More Details
CVE-2023-49238	In Gradle Enterprise before 2023.1, a remote attacker may be able to gain access to a new installation (in certain installation scenarios) because of a non-unique initial system user password. Although this password must be changed upon the first login, it is possible that an attacker logs in before the legitimate administrator logs in.	9.8	More Details
CVE-2023-51717	Dataiku DSS before 11.4.5 and 12.4.1 has Incorrect Access Control that could lead to a full authentication bypass.	9.8	More Details
CVE-2023-7220	A vulnerability was found in Totolink NR1800X 9.1.0u.6279_B20210910 and classified as critical. Affected by this issue is the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249854 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2023-49235	An issue was discovered in libremote_dbg.so on TRENDnet TV-IP1314PI 5.5.3 200714 devices. Filtering of debug information is mishandled during use of popen. Consequently, an attacker can bypass validation and execute a shell command.	9.8	More Details
CVE-2023-49236	A stack-based buffer overflow was discovered on TRENDnet TV-IP1314PI 5.5.3 200714 devices, leading to arbitrary command execution. This occurs because of lack of length validation during an sscanf of a user-entered scale field in the RTSP playback function of davinci.	9.8	More Details
CVE-2023-49237	An issue was discovered on TRENDnet TV-IP1314PI 5.5.3 200714 devices. Command injection can occur because the system function is used by davinci to unpack language packs without strict filtering of URL strings.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50585	Tenda A18 v15.13.07.09 was discovered to contain a stack overflow via the devName parameter in the formSetDeviceName function.	9.8	More Details
CVE-2023-49621	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.7). The "intermediate installation" system state of the affected application uses default credential with admin privileges. An attacker could use the credentials to gain complete control of the affected device.	9.8	More Details
CVE-2023-5347	An Improper Verification of Cryptographic Signature vulnerability in the update process of Korenix JetNet Series allows replacing the whole operating system including Trusted Executables. This issue affects JetNet devices older than firmware version 2024/01.	9.8	More Details
CVE-2023-7221	A vulnerability was found in Totolink T6 4.1.9cu.5241_B20210923. It has been classified as critical. This affects the function main of the file /cgi-bin/cstecgi.cgi?action=login of the component HTTP POST Request Handler. The manipulation of the argument v41 leads to buffer overflow. 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-249855. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2023-51277	nbviewer-app (aka Jupyter Notebook Viewer) before 0.1.6 has the get-task-allow entitlement for release builds.	9.8	More Details
CVE-2023-50027	SQL Injection vulnerability in Buy Addons baproductzoommagnifier module for PrestaShop versions 1.0.16 and before, allows remote attackers to escalate privileges and gain sensitive information via BaproductzoommagnifierZoomModuleFrontController::run() method.	9.8	More Details
CVE-2024-22087	route in main.c in Pico HTTP Server in C through f3b69a6 has an sprintf stack-based buffer overflow via a long URI, leading to remote code execution.	9.8	More Details
CVE-2023-50753	Online Notice Board System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'dd' parameter of the user/update_profile.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-49622	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'itemnameid' parameter of the material_bill.php?action=itemRelation resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-49624	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'cancelid' parameter of the material_bill.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-49625	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'id' parameter of the partylist_edit_submit.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49633	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'buyer_address' parameter of the buyer_detail_submit.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-49639	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'customer_details' parameter of the buyer_invoice_submit.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-49658	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'bank_details' parameter of the party_submit.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-49665	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'quantity[]' parameter of the submit_delivery_list.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2024-22086	handle_request in http.c in cherry through 4b877df has an sscanf stack-based buffer overflow via a long URI, leading to remote code execution.	9.8	More Details
CVE-2023-51784	Improper Control of Generation of Code ('Code Injection') vulnerability in Apache InLong.This issue affects Apache InLong: from 1.5.0 through 1.9.0, which could lead to Remote Code Execution. Users are advised to upgrade to Apache InLong's 1.10.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/9329	9.8	More Details
CVE-2023-49666	Billing Software v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'custmer_details' parameter of the submit_material_list.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-50743	Online Notice Board System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'dd' parameter of the registration.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-50090	Arbitrary File Write vulnerability in the saveReportFile method of ureport2 2.2.9 and before allows attackers to write arbitrary files and run arbitrary commands via crafted POST request.	9.8	More Details
CVE-2023-50752	Online Notice Board System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'e' parameter of the login.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-50862	Travel Website v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'hotelIDHidden' parameter of the booking.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-50863	Travel Website v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'hotelIDHidden' parameter of the generateReceipt.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-50864	Travel Website v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'hotelId' parameter of the hotelDetails.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50865	Travel Website v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'city' parameter of the hotelSearch.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-50866	Travel Website v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'username' parameter of the loginAction.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-50867	Travel Website v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'username' parameter of the signupAction.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-51154	Jizhicms v2.5 was discovered to contain an arbitrary file download vulnerability via the component /admin/c/PluginsController.php.	9.8	More Details
CVE-2023-51812	Tenda AX3 v16.03.12.11 was discovered to contain a remote code execution (RCE) vulnerability via the list parameter at /goform/SetNetControlList.	9.8	More Details
CVE-2024-22051	CommonMarker versions prior to 0.23.4 are at risk of an integer overflow vulnerability. This vulnerability can result in possibly unauthenticated remote attackers to cause heap memory corruption, potentially leading to an information leak or remote code execution, via parsing tables with marker rows that contain more than UINT16_MAX columns.	9.8	More Details
CVE-2023-49442	Deserialization of Untrusted Data in jeecgFormDemoController in JEECG 4.0 and earlier allows attackers to run arbitrary code via crafted POST request.	9.8	More Details
CVE-2023-52311	PaddlePaddle before 2.6.0 has a command injection in _wget_download. This resulted in the ability to execute arbitrary commands on the operating system.	9.6	More Details
CVE-2023-52310	PaddlePaddle before 2.6.0 has a command injection in get_online_pass_interval. This resulted in the ability to execute arbitrary commands on the operating system.	9.6	More Details
CVE-2023-52314	PaddlePaddle before 2.6.0 has a command injection in convert_shape_compare. This resulted in the ability to execute arbitrary commands on the operating system.	9.6	More Details
CVE-2023-37293	AMI’s SPx contains a vulnerability in the BMC where an Attacker may cause a stack-based buffer overflow via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	9.6	More Details
CVE-2023-39655	A host header injection vulnerability exists in the NPM package @perfood/couch-auth versions <= 0.20.0. By sending a specially crafted host header in the forgot password request, it is possible to send password reset links to users which, once clicked, lead to an attacker-controlled server and thus leak the password reset token. This may allow an attacker to reset other users' passwords and take over their accounts.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50253	Laf is a cloud development platform. In the Laf version design, the log uses communication with k8s to quickly retrieve logs from the container without the need for additional storage. However, in version 1.0.0-beta.13 and prior, this interface does not verify the permissions of the pod, which allows authenticated users to obtain any pod logs under the same namespace through this method, thereby obtaining sensitive information printed in the logs. As of time of publication, no known patched versions exist.	9.6	More Details
CVE-2023-52200	Cross-Site Request Forgery (CSRF), Deserialization of Untrusted Data vulnerability in Repute Infosystems ARMember – Membership Plugin, Content Restriction, Member Levels, User Profile & User signup.This issue affects ARMember – Membership Plugin, Content Restriction, Member Levels, User Profile & User signup: n/a.	9.6	More Details
CVE-2023-3043	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a stack-based buffer overflow via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	9.6	More Details
CVE-2023-52215	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in UkrSolution Simple Inventory Management – just scan barcode to manage products and orders. For WooCommerce.This issue affects Simple Inventory Management – just scan barcode to manage products and orders. For WooCommerce: from n/a through 1.5.1.	9.3	More Details
CVE-2023-52202	Deserialization of Untrusted Data vulnerability in SVNLabs Softwares HTML5 MP3 Player with Folder Feedburner Playlist Free.This issue affects HTML5 MP3 Player with Folder Feedburner Playlist Free: from n/a through 2.8.0.	9.1	More Details
CVE-2023-52205	Deserialization of Untrusted Data vulnerability in SVNLabs Softwares HTML5 SoundCloud Player with Playlist Free.This issue affects HTML5 SoundCloud Player with Playlist Free: from n/a through 2.8.0.	9.1	More Details
CVE-2023-52207	Deserialization of Untrusted Data vulnerability in SVNLabs Softwares HTML5 MP3 Player with Playlist Free.This issue affects HTML5 MP3 Player with Playlist Free: from n/a through 3.0.0.	9.1	More Details
CVE-2023-47211	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability.	9.1	More Details
CVE-2024-0057	NET, .NET Framework, and Visual Studio Security Feature Bypass Vulnerability	9.1	More Details
CVE-2024-0322	Out-of-bounds Read in GitHub repository gpac/gpac prior to 2.3-DEV.	9.1	More Details
CVE-2023-50982	Stud.IP 5.x through 5.3.3 allows XSS with resultant upload of executable files, because upload_action and edit_action in Admin_SmileysController do not check the file extension. This leads to remote code execution with the privileges of the www-data user. The fixed versions are 5.3.4, 5.2.6, 5.1.7, and 5.0.9.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-41288	An OS command injection vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following version: Video Station 5.7.2 (2023/11/23) and later	8.8	More Details
CVE-2024-0223	Heap buffer overflow in ANGLE in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-6140	The Essential Real Estate WordPress plugin before 4.4.0 does not prevent users with limited privileges on the site, like subscribers, from momentarily uploading malicious PHP files disguised as ZIP archives, which may lead to remote code execution.	8.8	More Details
CVE-2023-6528	The Slider Revolution WordPress plugin before 6.6.19 does not prevent users with at least the Author role from unserializing arbitrary content when importing sliders, potentially leading to Remote Code Execution.	8.8	More Details
CVE-2024-0222	Use after free in ANGLE in Google Chrome prior to 120.0.6099.199 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-6532	The WP Blogs' Planetarium WordPress plugin through 1.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	8.8	More Details
CVE-2024-21625	SideQuest is a place to get virtual reality applications for Oculus Quest. The SideQuest desktop application uses deep links with a custom protocol (`sidequest://`) to trigger actions in the application from its web contents. Because, prior to version 0.10.35, the deep link URLs were not sanitized properly in all cases, a one-click remote code execution can be achieved in cases when a device is connected, the user is presented with a malicious link and clicks it from within the application. As of version 0.10.35, the custom protocol links within the electron application are now being parsed and sanitized properly.	8.8	More Details
CVE-2023-50760	Online Notice Board System v1.0 is vulnerable to an Insecure File Upload vulnerability on the 'f' parameter of user/update_profile_pic.php page, allowing an authenticated attacker to obtain Remote Code Execution on the server hosting the application.	8.8	More Details
CVE-2024-0224	Use after free in WebAudio in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-21318	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-0225	Use after free in WebGPU in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-6845	The CommentTweets WordPress plugin through 0.6 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47890	pyLoad 0.5.0 is vulnerable to Unrestricted File Upload.	8.8	More Details
CVE-2023-52074	FlyCms v1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component system/site/webconfig_updagte.	8.8	More Details
CVE-2023-52073	FlyCms v1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /system/site/config_footer_updagte.	8.8	More Details
CVE-2023-52072	FlyCms v1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /system/site/userconfig_updagte.	8.8	More Details
CVE-2023-49251	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.7). The "intermediate installation" system state of the affected application allows an attacker to add their own login credentials to the device. This allows an attacker to remotely login as root and take control of the device even after the affected device is fully set up.	8.8	More Details
CVE-2024-20674	Windows Kerberos Security Feature Bypass Vulnerability	8.8	More Details
CVE-2023-39336	An unspecified SQL Injection vulnerability in Ivanti Endpoint Manager released prior to 2022 SU 5 allows an attacker with access to the internal network to execute arbitrary SQL queries and retrieve output without the need for authentication. Under specific circumstances, this may also lead to RCE on the core server.	8.8	More Details
CVE-2023-45722	HCL DRYiCE MyXalytics is impacted by path traversal arbitrary file read vulnerability because it uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory. The product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. Potential exploits can completely disrupt or take over the application.	8.8	More Details
CVE-2023-47994	An integer overflow vulnerability in LoadPixelDataRLE4 function in PluginBMP.cpp in Freeimage 3.18.0 allows attackers to obtain sensitive information, cause a denial of service and/or run arbitrary code.	8.8	More Details
CVE-2023-47992	An integer overflow vulnerability in FreeImageIO.cpp::_MemoryReadProc in FreeImage 3.18.0 allows attackers to obtain sensitive information, cause a denial-of-service attacks and/or run arbitrary code.	8.8	More Details
CVE-2023-29048	A component for parsing OXMF templates could be abused to execute arbitrary system commands that would be executed as the non-privileged runtime user. Users and attackers could run system commands with limited privilege to gain unauthorized access to confidential information and potentially violate integrity by modifying resources. The template engine has been reconfigured to deny execution of harmful commands on a system level. No publicly available exploits are known.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52150	Cross-Site Request Forgery (CSRF) vulnerability in Ovation S.R.L. Dynamic Content for Elementor.This issue affects Dynamic Content for Elementor: from n/a before 2.12.5.	8.8	More Details
CVE-2023-5880	When the Genie Company Aladdin Connect garage door opener (Retrofit-Kit Model ALDCM) is placed into configuration mode the web servers “Garage Door Control Module Setup” page is vulnerable to XSS via a broadcast SSID name containing malicious code with client side Java Script and/or HTML. This allows the attacker to inject malicious code with client side Java Script and/or HTML into the users' web browser.	8.8	More Details
CVE-2023-5235	The Ovic Responsive WPBakery WordPress plugin before 1.2.9 does not limit which options can be updated via some of its AJAX actions, which may allow attackers with a subscriber+ account to update blog options, such as 'users_can_register' and 'default_role'. It also unserializes user input in the process, which may lead to Object Injection attacks.	8.8	More Details
CVE-2024-0056	Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider Security Feature Bypass Vulnerability	8.7	More Details
CVE-2023-6600	The OMGF	GDPR/DSGVO Compliant, Faster Google Fonts. Easy. plugin for WordPress is vulnerable to unauthorized modification of data and Stored Cross-Site Scripting due to a missing capability check on the update_settings() function hooked via admin_init in all versions up to, and including, 5.7.9. This makes it possible for unauthenticated attackers to update the plugin's settings which can be used to inject Cross-Site Scripting payloads and delete entire directories. PLease note there were several attempted patched, and we consider 5.7.10 to be the most sufficiently patched.	8.6	More Details
CVE-2023-5376	An Improper Authentication vulnerability in Korenix JetNet TFTP allows abuse of this service. This issue affects JetNet devices older than firmware version 2024/01.	8.6	More Details
CVE-2023-52204	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Javik Randomize.This issue affects Randomize: from n/a through 1.4.3.	8.5	More Details
CVE-2024-21737	In SAP Application Interface Framework File Adapter - version 702, a high privilege user can use a function module to traverse through various layers and execute OS commands directly. By this, such user can control the behaviour of the application. This leads to considerable impact on confidentiality, integrity and availability.	8.4	More Details
CVE-2023-47145	IBM Db2 for Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow a local user to escalate their privileges to the SYSTEM user using the MSI repair functionality. IBM X-Force ID: 270402.	8.4	More Details
CVE-2023-50343	HCL DRYiCE MyXalytics is impacted by an Improper Access Control (Controller APIs) vulnerability. Certain API endpoints are accessible to Customer Admin Users that can allow access to sensitive information about other users.	8.3	More Details
CVE-2023-37294	AMI’s SPx contains a vulnerability in the BMC where an Attacker may cause a heap memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50930	An issue was discovered in savignano S/Notify before 4.0.2 for Jira. While an administrative user is logged on, the configuration settings of S/Notify can be modified via a CSRF attack. The injection could be initiated by the administrator clicking a malicious link in an email or by visiting a malicious website. If executed while an administrator is logged on to Jira, an attacker could exploit this to modify the configuration of the S/Notify app on that host. This can, in particular, lead to email notifications being no longer encrypted when they should be.	8.3	More Details
CVE-2023-37296	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a stack memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	8.3	More Details
CVE-2023-49722	Network port 8899 open in WiFi firmware of BCC101/BCC102/BCC50 products, that allows an attacker to connect to the device via same WiFi network.	8.3	More Details
CVE-2023-37297	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a heap memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	8.3	More Details
CVE-2023-50932	An issue was discovered in savignano S/Notify before 4.0.2 for Confluence. While an administrative user is logged on, the configuration settings of S/Notify can be modified via a CSRF attack. The injection could be initiated by the administrator clicking a malicious link in an email or by visiting a malicious website. If executed while an administrator is logged on to Confluence, an attacker could exploit this to modify the configuration of the S/Notify app on that host. This can, in particular, lead to email notifications being no longer encrypted when they should be.	8.3	More Details
CVE-2023-50931	An issue was discovered in savignano S/Notify before 2.0.1 for Bitbucket. While an administrative user is logged on, the configuration settings of S/Notify can be modified via a CSRF attack. The injection could be initiated by the administrator clicking a malicious link in an email or by visiting a malicious website. If executed while an administrator is logged on to Bitbucket, an attacker could exploit this to modify the configuration of the S/Notify app on that host. This can, in particular, lead to email notifications being no longer encrypted when they should be.	8.3	More Details
CVE-2023-37295	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause a heap memory corruption via an adjacent network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	8.3	More Details
CVE-2023-52307	Stack overflow in paddle.linalg.lu_unpack in PaddlePaddle before 2.6.0. This flaw can lead to a denial of service, or even more damage.	8.2	More Details
CVE-2023-45559	An issue in Tamaki_hamanoki Line v.13.6.1 allows attackers to send crafted notifications via leakage of the channel access token.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0213	A buffer overflow vulnerability in TA for Linux and TA for MacOS prior to 5.8.1 allows a local user to gain elevated permissions, or cause a Denial of Service (DoS), through exploiting a memory corruption issue in the TA service, which runs as root. This may also result in the disabling of event reporting to ePO, caused by failure to validate input from the file correctly.	8.2	More Details
CVE-2023-52309	Heap buffer overflow in paddle.repeat_interleave in PaddlePaddle before 2.6.0. This flaw can lead to a denial of service, information disclosure, or more damage is possible.	8.2	More Details
CVE-2023-5881	Unauthenticated access permitted to web interface page The Genie Company Aladdin Connect (Retrofit-Kit Model ALDCM) "Garage Door Control Module Setup" and modify the Garage door's SSID settings.	8.2	More Details
CVE-2023-50350	HCL DRYiCE MyXalytics is impacted by the use of a broken cryptographic algorithm for encryption, potentially giving an attacker ability to decrypt sensitive information.	8.2	More Details
CVE-2023-52304	Stack overflow in paddle.searchsorted in PaddlePaddle before 2.6.0. This flaw can lead to a denial of service, or even more damage.	8.2	More Details
CVE-2023-45724	HCL DRYiCE MyXalytics product is impacted by unauthenticated file upload vulnerability. The web application permits the upload of a certain file without requiring user authentication.	8.2	More Details
CVE-2023-50351	HCL DRYiCE MyXalytics is impacted by the use of an insecure key rotation mechanism which can allow an attacker to compromise the confidentiality or integrity of data.	8.2	More Details
CVE-2023-29051	User-defined OXMF templates could be used to access a limited part of the internal OX App Suite Java API. The existing switch to disable the feature by default was not effective in this case. Unauthorized users could discover and modify application state, including objects related to other users and contexts. We now make sure that the switch to disable user-generated templates by default works as intended and will remove the feature in future generations of the product. No publicly available exploits are known.	8.1	More Details
CVE-2024-20652	Windows HTML Platforms Security Feature Bypass Vulnerability	8.1	More Details
CVE-2024-20676	Azure Storage Mover Remote Code Execution Vulnerability	8.0	More Details
CVE-2024-20654	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21648	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The rollback action is missing a right protection, a user can rollback to a previous version of the page to gain rights they don't have anymore. The problem has been patched in XWiki 14.10.17, 15.5.3 and 15.8-rc-1 by ensuring that the rights are checked before performing the rollback.	8.0	More Details
CVE-2023-7208	A vulnerability classified as critical was found in Totolink X2000R_V2 2.0.0-B20230727.10434. This vulnerability affects the function formTmultiAP of the file /bin/boa. The manipulation leads to buffer overflow. VDB-249742 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.0	More Details
CVE-2023-38623	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `vindex_offset` array.	7.8	More Details
CVE-2023-39317	Multiple integer overflow vulnerabilities exist in the LXT2 num_dict_entries functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `string_lens` array.	7.8	More Details
CVE-2023-38618	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `rows` array.	7.8	More Details
CVE-2023-37922	Multiple arbitrary write vulnerabilities exist in the VCD sorted bsearch functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the arbitrary write when triggered via the vcd2lxt2 conversion utility.	7.8	More Details
CVE-2023-38583	A stack-based buffer overflow vulnerability exists in the LXT2 lxt2_rd_expand_integer_to_bits function of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2023-39443	Multiple out-of-bounds write vulnerabilities exist in the LXT2 parsing functionality of GTKWave 3.3.115. A specially-crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write perfomed by the prefix copy loop.	7.8	More Details
CVE-2023-37923	Multiple arbitrary write vulnerabilities exist in the VCD sorted bsearch functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the arbitrary write when triggered via the vcd2lxt conversion utility.	7.8	More Details
CVE-2023-39275	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `value` array.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37921	Multiple arbitrary write vulnerabilities exist in the VCD sorted bsearch functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the arbitrary write when triggered via the vcd2vzt conversion utility.	7.8	More Details
CVE-2023-37578	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the vcd2lxt conversion utility.	7.8	More Details
CVE-2023-39316	Multiple integer overflow vulnerabilities exist in the LXT2 num_dict_entries functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `string_pointers` array.	7.8	More Details
CVE-2023-38620	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `lsb` array.	7.8	More Details
CVE-2023-38619	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `msb` array.	7.8	More Details
CVE-2023-39274	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `len` array.	7.8	More Details
CVE-2023-38622	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `len` array.	7.8	More Details
CVE-2023-38621	Multiple integer overflow vulnerabilities exist in the VZT facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `flags` array.	7.8	More Details
CVE-2023-39273	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `flags` array.	7.8	More Details
CVE-2023-39272	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `lsb` array.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39271	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `msb` array.	7.8	More Details
CVE-2023-39270	Multiple integer overflow vulnerabilities exist in the LXT2 facgeometry parsing functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when allocating the `rows` array.	7.8	More Details
CVE-2023-39235	Multiple out-of-bounds write vulnerabilities exist in the VZT vzt_rd_process_block autosort functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when looping over `lt->num_time_ticks`.	7.8	More Details
CVE-2023-39234	Multiple out-of-bounds write vulnerabilities exist in the VZT vzt_rd_process_block autosort functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when looping over `lt->numrealfacs`.	7.8	More Details
CVE-2023-38657	An out-of-bounds write vulnerability exists in the LXT2 zlib block decompression functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2023-38649	Multiple out-of-bounds write vulnerabilities exist in the VZT vzt_rd_get_facname decompression functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write perfomed by the string copy loop.	7.8	More Details
CVE-2023-37577	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the vcd2lxt2 conversion utility.	7.8	More Details
CVE-2023-38648	Multiple out-of-bounds write vulnerabilities exist in the VZT vzt_rd_get_facname decompression functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write perfomed by the prefix copy loop.	7.8	More Details
CVE-2023-37443	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds read when triggered via the GUI's legacy VCD parsing code.	7.8	More Details
CVE-2023-37576	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the vcd2vzt conversion utility.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35996	Multiple improper array index validation vulnerabilities exist in the fstReaderIterBlocks2 tdelta functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the tdelta indexing when signal_lens is 0.	7.8	More Details
CVE-2023-35994	Multiple improper array index validation vulnerabilities exist in the fstReaderIterBlocks2 tdelta functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the tdelta initialization part.	7.8	More Details
CVE-2023-35989	An integer overflow vulnerability exists in the LXT2 zlib block allocation functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2023-35970	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 chain_table parsing functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the chain_table of the `FST_BL_VCDATA_DYN_ALIAS2` section type.	7.8	More Details
CVE-2023-35969	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 chain_table parsing functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the chain_table of `FST_BL_VCDATA` and `FST_BL_VCDATA_DYN_ALIAS` section types.	7.8	More Details
CVE-2023-35964	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns decompression in the `vcd2lxt` utility.	7.8	More Details
CVE-2023-35963	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns decompression in the `vcd2lxt2` utility.	7.8	More Details
CVE-2023-35962	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns decompression in the `vcd2vzt` utility.	7.8	More Details
CVE-2023-35961	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns decompression in `vcd_recorder_main`.	7.8	More Details
CVE-2023-35960	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns legacy decompression in `vcd_main`.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35959	Multiple OS command injection vulnerabilities exist in the decompression functionality of GTKWave 3.3.115. A specially crafted wave file can lead to arbitrary command execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns `.ghw` decompression.	7.8	More Details
CVE-2023-35958	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 VCDATA parsing functionality of GTKWave 3.3.115. A specially-crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the copy function `fstFread`.	7.8	More Details
CVE-2023-35957	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 VCDATA parsing functionality of GTKWave 3.3.115. A specially-crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the decompression function `uncompress`.	7.8	More Details
CVE-2023-35956	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 VCDATA parsing functionality of GTKWave 3.3.115. A specially-crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the decompression function `fastlz_decompress`.	7.8	More Details
CVE-2023-35955	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 VCDATA parsing functionality of GTKWave 3.3.115. A specially-crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the decompression function `LZ4_decompress_safe_partial`.	7.8	More Details
CVE-2023-35704	Multiple stack-based buffer overflow vulnerabilities exist in the FST LEB128 varint functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the fstReaderVarint32WithSkip function.	7.8	More Details
CVE-2023-35703	Multiple stack-based buffer overflow vulnerabilities exist in the FST LEB128 varint functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the fstReaderVarint64 function.	7.8	More Details
CVE-2023-35057	An integer overflow vulnerability exists in the LXT2 lxt2_rd_trace value elements allocation functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to memory corruption. A victim would need to open a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2023-35004	An integer overflow vulnerability exists in the VZT longest_len value allocation functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2023-34436	An out-of-bounds write vulnerability exists in the LXT2 num_time_table_entries functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2023-34087	An improper array index validation vulnerability exists in the EVCD var len parsing functionality of GTKWave 3.3.115. A specially crafted .evcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7224	OpenVPN Connect version 3.0 through 3.4.6 on macOS allows local users to execute code in external third party libraries using the DYLD_INSERT_LIBRARIES environment variable	7.8	More Details
CVE-2023-35995	Multiple improper array index validation vulnerabilities exist in the fstReaderIterBlocks2 tdelta functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the tdelta indexing when signal_lens is 1.	7.8	More Details
CVE-2023-50612	Insecure Permissions vulnerability in fit2cloud Cloud Explorer Lite version 1.4.1, allow local attackers to escalate privileges and obtain sensitive information via the cloud accounts parameter.	7.8	More Details
CVE-2023-37575	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the GUI's interactive VCD parsing code.	7.8	More Details
CVE-2023-35997	Multiple improper array index validation vulnerabilities exist in the fstReaderIterBlocks2 tdelta functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the tdelta indexing when signal_lens is 2 or more.	7.8	More Details
CVE-2023-34322	For migration as well as to work around kernels unaware of L1TF (see XSA-273), PV guests may be run in shadow paging mode. Since Xen itself needs to be mapped when PV guests run, Xen and shadowed PV guests run directly the respective shadow page tables. For 64-bit PV guests this means running on the shadow of the guest root page table. In the course of dealing with shortage of memory in the shadow pool associated with a domain, shadows of page tables may be torn down. This tearing down may include the shadow root page table that the CPU in question is presently running on. While a precaution exists to supposedly prevent the tearing down of the underlying live page table, the time window covered by that precaution isn't large enough.	7.8	More Details
CVE-2023-37574	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the GUI's legacy VCD parsing code.	7.8	More Details
CVE-2023-37573	Multiple use-after-free vulnerabilities exist in the VCD get_vartoken realloc functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the use-after-free when triggered via the GUI's recoder (default) VCD parsing code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34325	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] libfsimage contains parsing code for several filesystems, most of them based on grub-legacy code. libfsimage is used by pygrub to inspect guest disks. Pygrub runs as the same user as the toolstack (root in a priviledged domain). At least one issue has been reported to the Xen Security Team that allows an attacker to trigger a stack buffer overflow in libfsimage. After further analisys the Xen Security Team is no longer confident in the suitability of libfsimage when run against guest controlled input with super user priviledges. In order to not affect current deployments that rely on pygrub patches are provided in the resolution section of the advisory that allow running pygrub in deprivileged mode. CVE-2023-4949 refers to the original issue in the upstream grub project ("An attacker with local access to a system (either through a disk or external drive) can present a modified XFS partition to grub-legacy in such a way to exploit a memory corruption in grub's XFS file system implementation.") CVE-2023-34325 refers specifically to the vulnerabilities in Xen's copy of libfsimage, which is decended from a very old version of grub.	7.8	More Details
CVE-2023-34326	The caching invalidation guidelines from the AMD-Vi specification (48882—Rev 3.07-PUB—Oct 2022) is incorrect on some hardware, as devices will malfunction (see stale DMA mappings) if some fields of the DTE are updated but the IOMMU TLB is not flushed. Such stale DMA mappings can point to memory ranges not owned by the guest, thus allowing access to unindented memory regions.	7.8	More Details
CVE-2023-37447	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2lxt conversion utility.	7.8	More Details
CVE-2023-37446	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2lxt2 conversion utility.	7.8	More Details
CVE-2023-37445	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2vzt conversion utility.	7.8	More Details
CVE-2023-37444	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds read when triggered via the GUI's interactive VCD parsing code.	7.8	More Details
CVE-2022-3328	Race condition in snap-confine's must_mkdir_and_open_with_perms()	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37442	Multiple out-of-bounds read vulnerabilities exist in the VCD var definition section functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds read when triggered via the GUI's default VCD parsing code.	7.8	More Details
CVE-2023-37420	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2lxt conversion utility.	7.8	More Details
CVE-2023-37419	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2lxt2 conversion utility.	7.8	More Details
CVE-2023-37418	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the vcd2vzt conversion utility.	7.8	More Details
CVE-2023-37417	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the GUI's interactive VCD parsing code.	7.8	More Details
CVE-2023-37416	Multiple out-of-bounds write vulnerabilities exist in the VCD parse_valuechange portdump functionality of GTKWave 3.3.115. A specially crafted .vcd file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write when triggered via the GUI's legacy VCD parsing code.	7.8	More Details
CVE-2023-37282	An out-of-bounds write vulnerability exists in the VZT LZMA_Read dmem extraction functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2023-36916	Multiple integer overflow vulnerabilities exist in the FST fstReaderIterBlocks2 chain_table allocation functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the allocation of the `chain_table_lengths` array.	7.8	More Details
CVE-2023-36915	Multiple integer overflow vulnerabilities exist in the FST fstReaderIterBlocks2 chain_table allocation functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the allocation of the `chain_table` array.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36864	An integer overflow vulnerability exists in the fstReaderIterBlocks2 temp_signal_value_buf allocation functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2023-36861	An out-of-bounds write vulnerability exists in the VZT LZMA_read_varint functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2023-39444	Multiple out-of-bounds write vulnerabilities exist in the LXT2 parsing functionality of GTKWave 3.3.115. A specially-crafted .lxt2 file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the out-of-bounds write perfomed by the string copy loop.	7.8	More Details
CVE-2023-35702	Multiple stack-based buffer overflow vulnerabilities exist in the FST LEB128 varint functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the fstReaderVarint32 function.	7.8	More Details
CVE-2023-51746	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-20681	Windows Subsystem for Linux Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-49126	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-49127	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-49128	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-49129	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain a stack overflow vulnerability while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49130	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2023-49131	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2023-49132	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2023-51439	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-51745	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2021-3600	It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds information for 32 bit registers when performing div and mod operations. A local attacker could use this to possibly execute arbitrary code.	7.8	More Details
CVE-2024-20653	Microsoft Common Log File System Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-20656	Visual Studio Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-20658	Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20677	A security vulnerability exists in FBX that could lead to remote code execution. To mitigate this vulnerability, the ability to insert FBX files has been disabled in Word, Excel, PowerPoint and Outlook for Windows and Mac. Versions of Office that had this feature enabled will no longer have access to it. This includes Office 2019, Office 2021, Office LTSC for Mac 2021, and Microsoft 365. As of February 13, 2024, the ability to insert FBX files has also been disabled in 3D Viewer. 3D models in Office documents that were previously inserted from a FBX file will continue to work as expected unless the Link to File option was chosen at insert time. This change is effective as of the January 9, 2024 security update.	7.8	More Details
CVE-2024-20682	Windows Cryptographic Services Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-21633	Apktool is a tool for reverse engineering Android APK files. In versions 2.9.1 and prior, Apktool infers resource files' output path according to their resource names which can be manipulated by attacker to place files at desired location on the system Apktool runs on. Affected environments are those in which an attacker may write/overwrite any file that user has write access, and either user name is known or cwd is under user folder. Commit d348c43b24a9de350ff6e5bd610545a10c1fc712 contains a patch for this issue.	7.8	More Details
CVE-2024-20683	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-20686	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-0211	DOCSIS dissector crash in Wireshark 4.2.0 allows denial of service via packet injection or crafted capture file	7.8	More Details
CVE-2024-0210	Zigbee TLV dissector crash in Wireshark 4.2.0 allows denial of service via packet injection or crafted capture file	7.8	More Details
CVE-2024-0209	IEEE 1609.2 dissector crash in Wireshark 4.2.0, 4.0.0 to 4.0.11, and 3.6.0 to 3.6.19 allows denial of service via packet injection or crafted capture file	7.8	More Details
CVE-2024-0208	GVCP dissector crash in Wireshark 4.2.0, 4.0.0 to 4.0.11, and 3.6.0 to 3.6.19 allows denial of service via packet injection or crafted capture file	7.8	More Details
CVE-2024-0207	HTTP3 dissector crash in Wireshark 4.2.0 allows denial of service via packet injection or crafted capture file	7.8	More Details
CVE-2024-20698	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21309	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-21310	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-21325	Microsoft Printer Metadata Troubleshooter Tool Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-7032	A CWE-502: Deserialization of untrusted data vulnerability exists that could allow an attacker logged in with a user level account to gain higher privileges by providing a harmful serialized object.	7.8	More Details
CVE-2023-34332	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause an untrusted pointer to dereference by a local network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	7.8	More Details
CVE-2023-34333	AMI's SPx contains a vulnerability in the BMC where an Attacker may cause an untrusted pointer to dereference via a local network. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.	7.8	More Details
CVE-2023-49124	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2021-45465	A vulnerability has been identified in syngo fastView (All versions). The affected application lacks proper validation of user-supplied data when parsing BMP files. This could result in a write-what-where condition and an attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-15696)	7.8	More Details
CVE-2023-49123	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-6338	Uncontrolled search path vulnerabilities were reported in the Lenovo Universal Device Client (UDC) that could allow an attacker with local access to execute code with elevated privileges.	7.8	More Details
CVE-2023-49122	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-49121	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44120	A vulnerability has been identified in Spectrum Power 7 (All versions < V23Q4). The affected product's sudo configuration permits the local administrative account to execute several entries as root user. This could allow an authenticated local attacker to inject arbitrary code and gain root access.	7.8	More Details
CVE-2021-40367	A vulnerability has been identified in syngo fastView (All versions). The affected application lacks proper validation of user-supplied data when parsing DICOM files. This could result in an out-of-bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-15097)	7.8	More Details
CVE-2021-42028	A vulnerability has been identified in syngo fastView (All versions). The affected application lacks proper validation of user-supplied data when parsing BMP files. This could result in an out-of-bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-14860)	7.8	More Details
CVE-2023-6631	PowerSYSTEM Center versions 2020 Update 16 and prior contain a vulnerability that may allow an authorized local user to insert arbitrary code into the unquoted service path and escalate privileges.	7.8	More Details
CVE-2023-52206	Deserialization of Untrusted Data vulnerability in Live Composer Team Page Builder: Live Composer live-composer-page-builder.This issue affects Page Builder: Live Composer: from n/a through 1.5.25.	7.7	More Details
CVE-2023-42358	An issue was discovered in O-RAN Software Community ric-plt-e2mgr in the G-Release environment, allows remote attackers to cause a denial of service (DoS) via a crafted request to the E2Manager API component.	7.7	More Details
CVE-2023-50341	HCL DRYiCE MyXalytics is impacted by Improper Access Control (Obsolete web pages) vulnerability. Discovery of outdated and accessible web pages, reflects a "Missing Access Control" vulnerability, which could lead to inadvertent exposure of sensitive information and/or exposing a vulnerable endpoint.	7.6	More Details
CVE-2023-52142	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cool Plugins Events Shortcodes For The Events Calendar.This issue affects Events Shortcodes For The Events Calendar: from n/a through 2.3.1.	7.6	More Details
CVE-2023-52201	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Brian D. Goad pTypeConverter.This issue affects pTypeConverter: from n/a through 0.2.8.1.	7.6	More Details
CVE-2024-21747	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in weDevs WP ERP	Complete HR solution with recruitment & job listings	WooCommerce CRM & Accounting.This issue affects WP ERP	Complete HR solution with recruitment & job listings	WooCommerce CRM & Accounting: from n/a through 1.12.8.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29050	The optional "LDAP contacts provider" could be abused by privileged users to inject LDAP filter strings that allow to access content outside of the intended hierarchy. Unauthorized users could break confidentiality of information in the directory and potentially cause high load on the directory server, leading to denial of service. Encoding has been added for user-provided fragments that are used when constructing the LDAP query. No publicly available exploits are known.	7.6	More Details
CVE-2023-45723	HCL DRYiCE MyXalytics is impacted by path traversal vulnerability which allows file upload capability. Certain endpoints permit users to manipulate the path (including the file name) where these files are stored on the server.	7.6	More Details
CVE-2024-21312	.NET Framework Denial of Service Vulnerability	7.5	More Details
CVE-2023-6505	The Migrate WordPress Website & Backups WordPress plugin before 1.9.3 does not prevent directory listing in sensitive directories containing export files.	7.5	More Details
CVE-2023-51502	Authorization Bypass Through User-Controlled Key vulnerability in WooCommerce WooCommerce Stripe Payment Gateway.This issue affects WooCommerce Stripe Payment Gateway: from n/a through 7.6.1.	7.5	More Details
CVE-2024-22050	Path traversal in the static file service in Iodine less than 0.7.33 allows an unauthenticated, remote attacker to read files outside the public folder via malicious URLs.	7.5	More Details
CVE-2023-6750	The Clone WordPress plugin before 2.4.3 uses buffer files to store in-progress backup informations, which is stored at a publicly accessible, statically defined file path.	7.5	More Details
CVE-2023-52190	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in WP Swings Coupon Referral Program.This issue affects Coupon Referral Program: from n/a through 1.7.2.	7.5	More Details
CVE-2023-47473	Directory Traversal vulnerability in fuwushe.org iFair versions 23.8_ad0 and before allows an attacker to obtain sensitive information via a crafted script.	7.5	More Details
CVE-2024-20700	Windows Hyper-V Remote Code Execution Vulnerability	7.5	More Details
CVE-2023-50991	Buffer Overflow vulnerability in Tenda i29 versions 1.0 V1.0.0.5 and 1.0 V1.0.0.2, allows remote attackers to cause a denial of service (DoS) via the pingIp parameter in the pingSet function.	7.5	More Details
CVE-2024-21644	pyLoad is the free and open-source Download Manager written in pure Python. Any unauthenticated user can browse to a specific URL to expose the Flask config, including the `SECRET_KEY` variable. This issue has been patched in version 0.5.0b3.dev77.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6042	Any unauthenticated user may send e-mail from the site with any title or content to the admin	7.5	More Details
CVE-2024-21307	Remote Desktop Client Remote Code Execution Vulnerability	7.5	More Details
CVE-2023-7209	A vulnerability was found in Uniway Router up to 2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /boaform/device_reset.cgi of the component Device Reset Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249758 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.5	More Details
CVE-2023-6383	The Debug Log Manager WordPress plugin before 2.3.0 contains a Directory listing vulnerability was discovered, which allows you to download the debug log without authorization and gain access to sensitive data	7.5	More Details
CVE-2024-0241	encoded_id-rails versions before 1.0.0.beta2 are affected by an uncontrolled resource consumption vulnerability. A remote and unauthenticated attacker might cause a denial of service condition by sending an HTTP request with an extremely long "id" parameter.	7.5	More Details
CVE-2023-46929	An issue discovered in GPAC 2.3-DEV-rev605-gfc9e29089-master in MP4Box in gf_avc_change_vui /afltest/gpac/src/media_tools/av_parsers.c:6872:55 allows attackers to crash the application.	7.5	More Details
CVE-2022-2081	A vulnerability exists in the HCI Modbus TCP function included in the product versions listed above. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a lack of flood control which eventually if exploited causes an internal stack overflow in the HCI Modbus TCP function.	7.5	More Details
CVE-2023-51785	Deserialization of Untrusted Data vulnerability in Apache InLong.This issue affects Apache InLong: from 1.7.0 through 1.9.0, the attackers can make a arbitrary file read attack using mysql driver. Users are advised to upgrade to Apache InLong's 1.10.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/9331	7.5	More Details
CVE-2023-50256	Froxlor is open source server administration software. Prior to version 2.1.2, it was possible to submit the registration form with the essential fields, such as the username and password, left intentionally blank. This inadvertent omission allowed for a bypass of the mandatory field requirements (e.g. surname, company name) established by the system. Version 2.1.2 fixes this issue.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21634	Amazon Ion is a Java implementation of the Ion data notation. Prior to version 1.10.5, a potential denial-of-service issue exists in `ion-java` for applications that use `ion-java` to deserialize Ion text encoded data, or deserialize Ion text or binary encoded data into the `IonValue` model and then invoke certain `IonValue` methods on that in-memory representation. An actor could craft Ion data that, when loaded by the affected application and/or processed using the `IonValue` model, results in a `StackOverflowError` originating from the `ion-java` library. The patch is included in `ion-java` 1.10.5. As a workaround, do not load data which originated from an untrusted source or that could have been tampered with.	7.5	More Details
CVE-2023-39296	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later	7.5	More Details
CVE-2023-52143	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Naa986 WP Stripe Checkout.This issue affects WP Stripe Checkout: from n/a through 1.2.2.37.	7.5	More Details
CVE-2023-49252	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.7). The affected application allows IP configuration change without authentication to the device. This could allow an attacker to cause denial of service condition.	7.5	More Details
CVE-2024-21909	PeterO.Cbor versions 4.0.0 through 4.5.0 are vulnerable to a denial of service vulnerability. An attacker may trigger the denial of service condition by providing crafted data to the DecodeFromBytes or other decoding mechanisms in PeterO.Cbor. Depending on the usage of the library, an unauthenticated and remote attacker may be able to cause the denial of service condition.	7.5	More Details
CVE-2024-21907	Newtonsoft.Json before version 13.0.1 is affected by a mishandling of exceptional conditions vulnerability. Crafted data that is passed to the JsonConvert.DeserializeObject method may trigger a StackOverflow exception resulting in denial of service. Depending on the usage of the library, an unauthenticated and remote attacker may be able to cause the denial of service condition.	7.5	More Details
CVE-2023-50082	Aoyun Technology pbootcms V3.1.2 is vulnerable to Incorrect Access Control, allows remote attackers to gain sensitive information via session leakage allows a user to avoid logging into the backend management platform.	7.5	More Details
CVE-2023-37607	Directory Traversal in Automatic Systems SOC FL9600 FirstLane V06 lego_T04E00 allows a remote attacker to obtain sensitive information via csvServer.php?file= with a .. in the dir parameter.	7.5	More Details
CVE-2023-37608	An issue in Automatic Systems SOC FL9600 FirstLane V06 lego_T04E00 allows a remote attacker to obtain sensitive information because there is an automaticsystems super admin account with astech as its hardcoded password.	7.5	More Details
CVE-2023-27098	TP-Link Tapo APK up to v2.12.703 uses hardcoded credentials for access to the login panel.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21651	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A user able to attach a file to a page can post a malformed TAR file by manipulating file modification times headers, which when parsed by Tika, could cause a denial of service issue via CPU consumption. This vulnerability has been patched in XWiki 14.10.18, 15.5.3 and 15.8 RC1.	7.5	More Details
CVE-2024-21641	Flarum is open source discussion platform software. Prior to version 1.8.5, the Flarum `/logout` route includes a redirect parameter that allows any third party to redirect users from a (trusted) domain of the Flarum installation to redirect to any link. For logged-in users, the logout must be confirmed. Guests are immediately redirected. This could be used by spammers to redirect to a web address using a trusted domain of a running Flarum installation. The vulnerability has been fixed and published as flarum/core v1.8.5. As a workaround, some extensions modifying the logout route can remedy this issue if their implementation is safe.	7.5	More Details
CVE-2023-49961	WALLIX Bastion 7.x, 8.x, 9.x and 10.x and WALLIX Access Manager 3.x and 4.x have Incorrect Access Control which can lead to sensitive data exposure.	7.5	More Details
CVE-2024-21642	D-Tale is a visualizer for Pandas data structures. Users hosting versions D-Tale prior to 3.9.0 publicly can be vulnerable to server-side request forgery (SSRF), allowing attackers to access files on the server. Users should upgrade to version 3.9.0, where the `Load From the Web` input is turned off by default. The only workaround for versions earlier than 3.9.0 is to only host D-Tale to trusted users.	7.5	More Details
CVE-2024-20661	Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability	7.5	More Details
CVE-2024-20687	Microsoft AllJoyn API Denial of Service Vulnerability	7.5	More Details
CVE-2024-20672	.NET Denial of Service Vulnerability	7.5	More Details
CVE-2024-22125	Under certain conditions the Microsoft Edge browser extension (SAP GUI connector for Microsoft Edge) - version 1.0, allows an attacker to access highly sensitive information which would otherwise be restricted causing high impact on confidentiality.	7.4	More Details
CVE-2023-47560	An OS command injection vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following version: QuMagie 2.2.1 and later	7.4	More Details
CVE-2024-20697	Windows libarchive Remote Code Execution Vulnerability	7.3	More Details
CVE-2024-20696	Windows libarchive Remote Code Execution Vulnerability	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0307	A vulnerability was found in Kashipara Dynamic Lab Management System up to 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login_process.php. The manipulation of the argument password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249874 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-0294	A vulnerability, which was classified as critical, has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected by this issue is the function setUssd of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ussd leads to os command 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-249860. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-21735	SAP LT Replication Server - version S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108, does not perform necessary authorization checks. This could allow an attacker with high privileges to perform unintended actions, resulting in escalation of privileges, which has High impact on confidentiality, integrity and availability of the system.	7.3	More Details
CVE-2024-0299	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been declared as critical. Affected by this vulnerability is the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249865 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-0298	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been classified as critical. Affected is the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-249864. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-0297	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as critical. This issue affects the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to os command 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-249863. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-0296	A vulnerability has been found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as critical. This vulnerability affects the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument host_time leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249862 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0295	A vulnerability, which was classified as critical, was found in Totolink LR1200GB 9.1.0u.6619_B20230130. This affects the function setWanCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249861 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-0306	A vulnerability was found in Kashipara Dynamic Lab Management System up to 1.0. It has been classified as critical. This affects an unknown part of the file /admin/admin_login_process.php. The manipulation of the argument admin_password 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-249873 was assigned to this vulnerability.	7.3	More Details
CVE-2024-0352	A vulnerability classified as critical was found in Likeshop up to 2.5.7.20210311. This vulnerability affects the function FileServer::userFormImage of the file server/application/api/controller/File.php of the component HTTP POST Request Handler. The manipulation of the argument file leads to unrestricted upload. 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-250120.	7.3	More Details
CVE-2023-7210	A vulnerability was found in OneNav up to 0.9.33. It has been classified as critical. This affects an unknown part of the file /index.php?c=api of the component API. The manipulation of the argument X-Token leads to improper authentication. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249765 was assigned to this vulnerability.	7.3	More Details
CVE-2024-0264	A vulnerability was found in SourceCodester Clinic Queuing System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /LoginRegistration.php. The manipulation of the argument formToken leads to authorization bypass. 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-249820.	7.3	More Details
CVE-2024-0247	A vulnerability classified as critical was found in CodeAstro Online Food Ordering System 1.0. This vulnerability affects unknown code of the file /admin/ of the component Admin Panel. The manipulation of the argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249778 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-0267	A vulnerability classified as critical was found in Kashipara Hospital Management System up to 1.0. Affected by this vulnerability is an unknown functionality of the file login.php of the component Parameter Handler. The manipulation of the argument email/password 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-249823.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0268	A vulnerability, which was classified as critical, has been found in Kashipara Hospital Management System up to 1.0. Affected by this issue is some unknown functionality of the file registration.php. The manipulation of the argument name/email/pass/gender/age/city 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-249824.	7.3	More Details
CVE-2023-7027	The POST SMTP Mailer – Email log, Delivery Failure Notifications and Best Mail SMTP for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'device' header in all versions up to, and including, 2.8.7 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-2023-7219	A vulnerability has been found in Totolink N350RT 9.3.5u.6139_B202012 and classified as critical. Affected by this vulnerability is the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument http_host leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249853 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2023-50922	An issue was discovered on GL.iNet devices through 4.5.0. Attackers who are able to steal the AdminToken cookie can execute arbitrary code by uploading a crontab-formatted file to a specific directory and waiting for its execution. This affects A1300 4.4.6, AX1800 4.4.6, AXT1800 4.4.6, MT3000 4.4.6, MT2500 4.4.6, MT6000 4.5.0, MT1300 4.3.7, MT300N-V2 4.3.7, AR750S 4.3.7, AR750 4.3.7, AR300M 4.3.7, and B1300 4.3.7.	7.2	More Details
CVE-2023-50162	SQL injection vulnerability in EmpireCMS v7.5, allows remote attackers to execute arbitrary code and obtain sensitive information via the DoExecSql function.	7.2	More Details
CVE-2023-7218	A vulnerability, which was classified as critical, was found in Totolink N350RT 9.3.5u.6139_B202012. Affected is the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to stack-based buffer overflow. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-249852. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2023-5957	The Ni Purchase Order(PO) For WooCommerce WordPress plugin through 1.2.1 does not validate logo and signature image files uploaded in the settings, allowing high privileged user to upload arbitrary files to the web server, triggering an RCE vulnerability by uploading a web shell.	7.2	More Details
CVE-2023-7222	A vulnerability was found in Totolink X2000R 1.0.0-B20221212.1452. It has been declared as critical. This vulnerability affects the function formTmultiAP of the file /bin/boa of the component HTTP POST Request Handler. The manipulation of the argument submit-url leads to buffer overflow. 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-249856. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51441	** UNSUPPORTED WHEN ASSIGNED ** Improper Input Validation vulnerability in Apache Axis allowed users with access to the admin service to perform possible SSRF This issue affects Apache Axis: through 1.3. As Axis 1 has been EOL we recommend you migrate to a different SOAP engine, such as Apache Axis 2/Java. Alternatively you could use a build of Axis with the patch from https://github.com/apache/axis-axis1-java/commit/685c309febc64aa393b2d64a05f90e7eb9f73e06 applied. The Apache Axis project does not expect to create an Axis 1.x release fixing this problem, though contributors that would like to work towards this are welcome.	7.2	More Details
CVE-2023-52196	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Phil Ewels CPT Bootstrap Carousel allows Reflected XSS.This issue affects CPT Bootstrap Carousel: from n/a through 1.12.	7.1	More Details
CVE-2024-0206	A symbolic link manipulation vulnerability in Trellix Anti-Malware Engine prior to the January 2024 release allows an authenticated local user to potentially gain an escalation of privileges. This was achieved by adding an entry to the registry under the Trellix ENS registry folder with a symbolic link to files that the user wouldn't normally have permission to. After a scan, the Engine would follow the links and remove the files	7.1	More Details
CVE-2023-52213	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VideoWhisper Rate Star Review – AJAX Reviews for Content, with Star Ratings allows Reflected XSS.This issue affects Rate Star Review – AJAX Reviews for Content, with Star Ratings: from n/a through 1.5.1.	7.1	More Details
CVE-2023-50342	HCL DRYiCE MyXalytics is impacted by an Insecure Direct Object Reference (IDOR) vulnerability. A user can obtain certain details about another user as a result of improper access control.	7.1	More Details
CVE-2022-48618	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.1, watchOS 9.2, iOS 16.2 and iPadOS 16.2, tvOS 16.2. An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. Apple is aware of a report that this issue may have been exploited against versions of iOS released before iOS 15.7.1.	7.0	More Details
CVE-2023-32650	An integer overflow vulnerability exists in the FST_BL_GEOM parsing maxhandle functionality of GTKWave 3.3.115, when compiled as a 32-bit binary. A specially crafted .fst file can lead to memory corruption. A victim would need to open a malicious file to trigger this vulnerability.	7.0	More Details
CVE-2022-36763	EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.	7.0	More Details
CVE-2022-36764	EDK2 is susceptible to a vulnerability in the Tcg2MeasurePeImage() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.	7.0	More Details
CVE-2024-20657	Windows Group Policy Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35128	An integer overflow vulnerability exists in the fstReaderIterBlocks2 time_table tsec_nitems functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to memory corruption. A victim would need to open a malicious file to trigger this vulnerability.	7.0	More Details
CVE-2023-36747	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 fstWritex len functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the handling of `len` in `fstWritex` when `beg_time` does not match the start of the time table.	7.0	More Details
CVE-2022-36765	EDK2 is susceptible to a vulnerability in the CreateHob() function, allowing a user to trigger a integer overflow to buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.	7.0	More Details
CVE-2023-39413	Multiple integer underflow vulnerabilities exist in the LXT2 lxt2_rd_iter_radix shift operation functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer underflow when performing the left shift operation.	7.0	More Details
CVE-2023-6270	A flaw was found in the ATA over Ethernet (AoE) driver in the Linux kernel. The aoecmd_cfg_pkts() function improperly updates the refcnt on `struct net_device`, and a use-after-free can be triggered by racing between the free on the struct and the access through the `skbtxq` global queue. This could lead to a denial of service condition or potential code execution.	7.0	More Details
CVE-2023-38650	Multiple integer overflow vulnerabilities exist in the VZT vzt_rd_block_vch_decode times parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when num_time_ticks is not zero.	7.0	More Details
CVE-2023-38651	Multiple integer overflow vulnerabilities exist in the VZT vzt_rd_block_vch_decode times parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when num_time_ticks is zero.	7.0	More Details
CVE-2023-35992	An integer overflow vulnerability exists in the FST fstReaderIterBlocks2 vesc allocation functionality of GTKWave 3.3.115, when compiled as a 32-bit binary. A specially crafted .fst file can lead to memory corruption. A victim would need to open a malicious file to trigger this vulnerability.	7.0	More Details
CVE-2023-38652	Multiple integer overflow vulnerabilities exist in the VZT vzt_rd_block_vch_decode dict parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when num_time_ticks is not zero.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36746	Multiple heap-based buffer overflow vulnerabilities exist in the fstReaderIterBlocks2 fstWritex len functionality of GTKWave 3.3.115. A specially crafted .fst file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the handling of `len` in `fstWritex` when parsing the time table.	7.0	More Details
CVE-2023-38653	Multiple integer overflow vulnerabilities exist in the VZT vzt_rd_block_vch_decode dict parsing functionality of GTKWave 3.3.115. A specially crafted .vzt file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer overflow when num_time_ticks is zero.	7.0	More Details
CVE-2023-39414	Multiple integer underflow vulnerabilities exist in the LXT2 lxt2_rd_iter_radix shift operation functionality of GTKWave 3.3.115. A specially crafted .lxt2 file can lead to memory corruption. A victim would need to open a malicious file to trigger these vulnerabilities.This vulnerability concerns the integer underflow when performing the right shift operation.	7.0	More Details
CVE-2023-5138	Glitch detection is not enabled by default for the CortexM33 core in Silicon Labs secure vault high parts EFx32xG2xB, except EFR32xG21B.	6.8	More Details
CVE-2024-20803	Improper authentication vulnerability in Bluetooth pairing process prior to SMR Jan-2024 Release 1 allows remote attackers to establish pairing process without user interaction.	6.8	More Details
CVE-2024-21319	Microsoft Identity Denial of service vulnerability	6.8	More Details
CVE-2023-5879	Users' product account authentication data was stored in clear text in The Genie Company Aladdin Connect Mobile Application Version 5.65 Build 2075 (and below) on Android Devices. This allows the attacker, with access to the android device, to potentially retrieve users' clear text authentication credentials.	6.8	More Details
CVE-2023-41776	There is a local privilege escalation vulnerability of ZTE's ZXCLOUD iRAI.Attackers with regular user privileges can create a fake process, and to escalate local privileges.	6.7	More Details
CVE-2023-41784	Permissions and Access Control Vulnerability in ZTE Red Magic 8 Pro	6.6	More Details
CVE-2023-39294	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later	6.6	More Details
CVE-2024-20655	Microsoft Online Certificate Status Protocol (OCSP) Remote Code Execution Vulnerability	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42797	A vulnerability has been identified in CP-8031 MASTER MODULE (All versions < CPCI85 V05.20), CP-8050 MASTER MODULE (All versions < CPCI85 V05.20). The network configuration service of affected devices contains a flaw in the conversion of ipv4 addresses that could lead to an uninitialized variable being used in succeeding validation steps. By uploading specially crafted network configuration, an authenticated remote attacker could be able to inject commands that are executed on the device with root privileges during device startup.	6.6	More Details
CVE-2024-20666	BitLocker Security Feature Bypass Vulnerability	6.6	More Details
CVE-2023-6129	Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used. This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue.	6.5	More Details
CVE-2024-22165	In Splunk Enterprise Security (ES) versions lower than 7.1.2, an attacker can create a malformed Investigation to perform a denial of service (DoS). The malformed investigation prevents the generation and rendering of the Investigations manager until it is deleted. The vulnerability requires an authenticated session and access to create an Investigation. It only affects the availability of the Investigations manager, but without the manager, the Investigations functionality becomes unusable for most users.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21631	Vapor is an HTTP web framework for Swift. Prior to version 4.90.0, Vapor's `vapor_urlparser_parse` function uses `uint16_t` indexes when parsing a URI's components, which may cause integer overflows when parsing untrusted inputs. This vulnerability does not affect Vapor directly but could impact applications relying on the URI type for validating user input. The URI type is used in several places in Vapor. A developer may decide to use URI to represent a URL in their application (especially if that URL is then passed to the HTTP Client) and rely on its public properties and methods. However, URI may fail to properly parse a valid (albeit abnormally long) URL, due to string ranges being converted to 16-bit integers. An attacker may use this behavior to trick the application into accepting a URL to an untrusted destination. By padding the port number with zeros, an attacker can cause an integer overflow to occur when the URL authority is parsed and, as a result, spoof the host. Version 4.90.0 contains a patch for this issue. As a workaround, validate user input before parsing as a URI or, if possible, use Foundation's `URL` and `URLComponents` utilities.	6.5	More Details
CVE-2023-30617	Kruise provides automated management of large-scale applications on Kubernetes. Starting in version 0.8.0 and prior to versions 1.3.1, 1.4.1, and 1.5.2, an attacker who has gained root privilege of the node that kruise-daemon run can leverage the kruise-daemon pod to list all secrets in the entire cluster. After that, the attacker can leverage the "captured" secrets (e.g. the kruise-manager service account token) to gain extra privileges such as pod modification. Versions 1.3.1, 1.4.1, and 1.5.2 fix this issue. A workaround is available. For users that do not require imagepulljob functions, they can modify kruise-daemon-role to drop the cluster level secret get/list privilege.	6.5	More Details
CVE-2023-46738	CubeFS is an open-source cloud-native file storage system. A security vulnerability was found in CubeFS HandlerNode in versions prior to 3.3.1 that could allow authenticated users to send maliciously-crafted requests that would crash the ObjectNode and deny other users from using it. The root cause was improper handling of incoming HTTP requests that could allow an attacker to control the ammount of memory that the ObjectNode would allocate. A malicious request could make the ObjectNode allocate more memory that the machine had available, and the attacker could exhaust memory by way of a single malicious request. An attacker would need to be authenticated in order to invoke the vulnerable code with their malicious request and have permissions to delete objects. In addition, the attacker would need to know the names of existing buckets of the CubeFS deployment - otherwise the request would be rejected before it reached the vulnerable code. As such, the most likely attacker is an inside user or an attacker that has breached the account of an existing user in the cluster. The issue has been patched in v3.3.1. There is no other mitigation besides upgrading.	6.5	More Details
CVE-2023-46739	CubeFS is an open-source cloud-native file storage system. A vulnerability was found during in the CubeFS master component in versions prior to 3.3.1 that could allow an untrusted attacker to steal user passwords by carrying out a timing attack. The root case of the vulnerability was that CubeFS used raw string comparison of passwords. The vulnerable part of CubeFS was the UserService of the master component. The UserService gets instantiated when starting the server of the master component. The issue has been patched in v3.3.1. For impacted users, there is no other way to mitigate the issue besides upgrading.	6.5	More Details
CVE-2023-52125	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly iframe allows Stored XSS.This issue affects iframe: from n/a through 4.8.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52124	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShapedPlugin LLC WP Tabs – Responsive Tabs Plugin for WordPress allows Stored XSS.This issue affects WP Tabs – Responsive Tabs Plugin for WordPress: from n/a through 2.2.0.	6.5	More Details
CVE-2023-46740	CubeFS is an open-source cloud-native file storage system. Prior to version 3.3.1, CubeFS used an insecure random string generator to generate user-specific, sensitive keys used to authenticate users in a CubeFS deployment. This could allow an attacker to predict and/or guess the generated string and impersonate a user thereby obtaining higher privileges. When CubeFS creates new users, it creates a piece of sensitive information for the user called the “accessKey”. To create the "accesKey", CubeFS uses an insecure string generator which makes it easy to guess and thereby impersonate the created user. An attacker could leverage the predictable random string generator and guess a users access key and impersonate the user to obtain higher privileges. The issue has been fixed in v3.3.1. There is no other mitigation than to upgrade.	6.5	More Details
CVE-2023-6540	A vulnerability was reported in the Lenovo Browser Mobile and Lenovo Browser HD Apps for Android that could allow an attacker to craft a payload that could result in the disclosure of sensitive information.	6.5	More Details
CVE-2023-6830	The Formidable Forms plugin for WordPress is vulnerable to HTML injection in versions up to, and including, 6.7. This vulnerability allows unauthenticated users to inject arbitrary HTML code into form fields. When the form data is viewed by an administrator in the Entries View Page, the injected HTML code is rendered, potentially leading to admin area defacement or redirection to malicious websites.	6.5	More Details
CVE-2023-6733	The WP-Members Membership Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.4.8 via the wpmem_field shortcode. This makes it possible for authenticated attackers, with contributor access and above, to extract sensitive data including user emails, password hashes, usernames, and more.	6.5	More Details
CVE-2023-29962	S-CMS v5.0 was discovered to contain an arbitrary file read vulnerability.	6.5	More Details
CVE-2023-52198	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michiel van Eerd Private Google Calendars allows Stored XSS.This issue affects Private Google Calendars: from n/a through 20231125.	6.5	More Details
CVE-2023-52178	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MojofyWP WP Affiliate Disclosure allows Stored XSS.This issue affects WP Affiliate Disclosure: from n/a through 1.2.7.	6.5	More Details
CVE-2024-21744	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mapster Technology Inc. Mapster WP Maps allows Stored XSS.This issue affects Mapster WP Maps: from n/a through 1.2.38.	6.5	More Details
CVE-2024-21745	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Laybuy Laybuy Payment Extension for WooCommerce allows Stored XSS.This issue affects Laybuy Payment Extension for WooCommerce: from n/a through 5.3.9.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52271	The wsftprm.sys kernel driver 2.0.0.0 in Topaz Antifraud allows low-privileged attackers to kill any (Protected Process Light) process via an IOCTL (which will be named at a later time).	6.5	More Details
CVE-2023-39853	SQL Injection vulnerability in Dzzoffice version 2.01, allows remote attackers to obtain sensitive information via the doobj and doevent parameters in the Network Disk backend module.	6.5	More Details
CVE-2023-6139	The Essential Real Estate WordPress plugin before 4.4.0 does not apply proper capability checks on its AJAX actions, which among other things, allow attackers with a subscriber account to conduct Denial of Service attacks.	6.5	More Details
CVE-2024-20660	Microsoft Message Queuing Information Disclosure Vulnerability	6.5	More Details
CVE-2023-50948	IBM Storage Fusion HCI 2.1.0 through 2.6.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 275671.	6.5	More Details
CVE-2024-21320	Windows Themes Spoofing Vulnerability	6.5	More Details
CVE-2024-21314	Microsoft Message Queuing Information Disclosure Vulnerability	6.5	More Details
CVE-2023-6476	A flaw was found in CRI-O that involves an experimental annotation leading to a container being unconfined. This may allow a pod to specify and get any amount of memory/cpu, circumventing the kubernetes scheduler and potentially resulting in a denial of service in the node.	6.5	More Details
CVE-2023-47993	A Buffer out-of-bound read vulnerability in Exif.cpp::ReadInt32 in FreeImage 3.18.0 allows attackers to cause a denial-of-service.	6.5	More Details
CVE-2024-20663	Windows Message Queuing Client (MSMQC) Information Disclosure	6.5	More Details
CVE-2023-47996	An integer overflow vulnerability in Exif.cpp::jpeg_read_exif_dir in FreeImage 3.18.0 allows attackers to obtain information and cause a denial of service.	6.5	More Details
CVE-2023-47995	Memory Allocation with Excessive Size Value discovered in BitmapAccess.cpp::FreeImage_AllocateBitmap in FreeImage 3.18.0 allows attackers to cause a denial of service.	6.5	More Details
CVE-2024-20680	Windows Message Queuing Client (MSMQC) Information Disclosure	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20690	Windows Nearby Sharing Spoofing Vulnerability	6.5	More Details
CVE-2024-20664	Microsoft Message Queuing Information Disclosure Vulnerability	6.5	More Details
CVE-2024-21736	SAP S/4HANA Finance for (Advanced Payment Management) - versions SAPSCORE 128, S4CORE 107, does not perform necessary authorization checks. A function import could be triggered allowing the attacker to create in-house bank accounts leading to low impact on the confidentiality of the application.	6.4	More Details
CVE-2023-6986	The EmbedPress – Embed PDF, YouTube, Google Docs, Vimeo, Wistia Videos, Audios, Maps & Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's embed_oembed_html shortcode in all versions up to 3.9.5 (exclusive) due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-7044	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom ID in all versions up to, and including, 5.9.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor access and higher to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-6801	The RSS Aggregator by Feedzy – Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 4.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-6747	The Best WordPress Gallery Plugin – FooGallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom attributes in all versions up to, and including, 2.3.3 due to insufficient input sanitization and output escaping. This makes it possible for contributors and above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-6524	The MapPress Maps for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the map title parameter in all versions up to and including 2.88.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor access or higher to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-41780	There is an unsafe DLL loading vulnerability in ZTE ZXCLOUD iRAI. Due to the program failed to adequately validate the user's input, an attacker could exploit this vulnerability to escalate local privileges.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0304	A vulnerability has been found in Youke365 up to 1.5.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /app/api/controller/collect.php. The manipulation of the argument url leads to server-side request forgery. 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-249871.	6.3	More Details
CVE-2024-0303	A vulnerability, which was classified as critical, was found in Youke365 up to 1.5.3. Affected is an unknown function of the file /app/api/controller/caiji.php of the component Parameter Handler. The manipulation of the argument url leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-249870 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0302	A vulnerability, which was classified as critical, has been found in fhs-opensource iparking 1.5.22.RELEASE. This issue affects some unknown processing of the file /vueLogin. The manipulation leads to deserialization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249869 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0301	A vulnerability classified as critical was found in fhs-opensource iparking 1.5.22.RELEASE. This vulnerability affects the function getData of the file src/main/java/com/xhb/pay/action/PayTempOrderAction.java. The manipulation 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-249868.	6.3	More Details
CVE-2024-0300	A vulnerability was found in Byzoro Smart S150 Management Platform up to 20240101. It has been rated as critical. Affected by this issue is some unknown functionality of the file /useratte/userattestation.php of the component HTTP POST Request Handler. The manipulation of the argument web_img leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249866 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-0289	A vulnerability classified as critical was found in Kashipara Food Management System 1.0. This vulnerability affects unknown code of the file stock_entry_submit.php. The manipulation of the argument itemype leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-249850 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-36352	Missing Authorization vulnerability in Profilegrid ProfileGrid – User Profiles, Memberships, Groups and Communities.This issue affects ProfileGrid – User Profiles, Memberships, Groups and Communities: from n/a through 5.0.3.	6.3	More Details
CVE-2023-52129	Cross-Site Request Forgery (CSRF) vulnerability in Michael Winkler teachPress.This issue affects teachPress: from n/a through 9.0.4.	6.3	More Details
CVE-2024-0290	A vulnerability, which was classified as critical, has been found in Kashipara Food Management System 1.0. This issue affects some unknown processing of the file stock_edit.php. The manipulation of the argument item_type 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-249851.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7213	A vulnerability classified as critical was found in Totolink N350RT 9.3.5u.6139_B20201216. Affected by this vulnerability is the function main of the file /cgi-bin/cstecgi.cgi?action=login&flag=1 of the component HTTP POST Request Handler. The manipulation of the argument v33 leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249769 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-0293	A vulnerability classified as critical was found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected by this vulnerability is the function setUploadSetting of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to os command 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-249859. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-0292	A vulnerability classified as critical has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected is the function setOpModeCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-249858 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-0287	A vulnerability was found in Kashipara Food Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file itemBillPdf.php. The manipulation of the argument printid 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-249848.	6.3	More Details
CVE-2024-0291	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been rated as critical. This issue affects the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249857 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-0288	A vulnerability classified as critical has been found in Kashipara Food Management System 1.0. This affects an unknown part of the file rawstock_used_damaged_submit.php. The manipulation of the argument product_name 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-249849 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0281	A vulnerability was found in Kashipara Food Management System up to 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file loginCheck.php. The manipulation of the argument password 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-249836.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0342	A vulnerability classified as critical has been found in Inis up to 2.0.1. Affected is an unknown function of the file /app/api/controller/default/Sqlite.php. The manipulation of the argument sql leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-250110 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0276	A vulnerability classified as critical has been found in Kashipara Food Management System up to 1.0. This affects an unknown part of the file rawstock_used_damaged_smt.php. The manipulation of the argument product_name 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-249831.	6.3	More Details
CVE-2024-0265	A vulnerability was found in SourceCodester Clinic Queuing System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /index.php of the component GET Parameter Handler. The manipulation of the argument page leads to file inclusion. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249821 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0270	A vulnerability, which was classified as critical, was found in Kashipara Food Management System up to 1.0. This affects an unknown part of the file item_list_submit.php. The manipulation of the argument item_name 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-249825 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0271	A vulnerability has been found in Kashipara Food Management System up to 1.0 and classified as critical. This vulnerability affects unknown code of the file addmaterial_edit.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-249826 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0272	A vulnerability was found in Kashipara Food Management System up to 1.0 and classified as critical. This issue affects some unknown processing of the file addmaterialsubmit.php. The manipulation of the argument material_name 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-249827.	6.3	More Details
CVE-2024-0273	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been classified as critical. Affected is an unknown function of the file addwaste_entry.php. The manipulation of the argument item_name 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-249828.	6.3	More Details
CVE-2023-41289	An OS command injection vulnerability has been reported to affect QcalAgent. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following version: QcalAgent 1.1.8 and later	6.3	More Details
CVE-2024-0274	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file billAjax.php. The manipulation of the argument item_name 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-249829 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0280	A vulnerability has been found in Kashipara Food Management System up to 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file item_type_submit.php. The manipulation of the argument type_name 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-249835.	6.3	More Details
CVE-2024-0275	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file item_edit_submit.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-249830 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-7214	A vulnerability, which was classified as critical, has been found in Totolink N350RT 9.3.5u.6139_B20201216. Affected by this issue is the function main of the file /cgi-bin/cstecgi.cgi?action=login of the component HTTP POST Request Handler. The manipulation of the argument v8 leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249770 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-0279	A vulnerability, which was classified as critical, was found in Kashipara Food Management System up to 1.0. Affected is an unknown function of the file item_list_edit.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-249834 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0308	A vulnerability was found in Inis up to 2.0.1. It has been rated as critical. This issue affects some unknown processing of the file app/api/controller/default/Proxy.php. The manipulation of the argument p_url leads to server-side request forgery. 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-249875.	6.3	More Details
CVE-2024-0277	A vulnerability classified as critical was found in Kashipara Food Management System up to 1.0. This vulnerability affects unknown code of the file party_submit.php. The manipulation of the argument party_name 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-249832.	6.3	More Details
CVE-2024-0278	A vulnerability, which was classified as critical, has been found in Kashipara Food Management System up to 1.0. This issue affects some unknown processing of the file partylist_edit_submit.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249833 was assigned to this vulnerability.	6.3	More Details
CVE-2024-20806	Improper access control in Notification service prior to SMR Jan-2024 Release 1 allows local attacker to access notification data.	6.2	More Details
CVE-2024-21911	TinyMCE versions before 5.6.0 are affected by a stored cross-site scripting vulnerability. An unauthenticated and remote attacker could insert crafted HTML into the editor resulting in arbitrary JavaScript execution in another user's browser.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21636	view_component is a framework for building reusable, testable, and encapsulated view components in Ruby on Rails. Versions prior to 3.9.0 and 2.83.0 have a cross-site scripting vulnerability that has the potential to impact anyone rendering a component directly from a controller with the view_component gem. Note that only components that define a `#call` method (i.e. instead of using a sidecar template) are affected. The return value of the `#call` method is not sanitized and can include user-defined content. In addition, the return value of the `#output_postamble` methodis not sanitized, which can also lead to cross-site scripting issues. Versions 3.9.0 and 2.83.0 have been released and fully mitigate both the `#call` and the `#output_postamble` vulnerabilities. As a workaround, sanitize the return value of `#call`.	6.1	More Details
CVE-2023-6161	The WP Crowdfunding WordPress plugin before 2.1.9 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-6621	The POST SMTP WordPress plugin before 2.8.7 does not sanitise and escape the msg parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	6.1	More Details
CVE-2023-6529	The WP VR WordPress plugin before 8.3.15 does not authorisation and CSRF in a function hooked to admin_init, allowing unauthenticated users to downgrade the plugin, thus leading to Reflected or Stored XSS, as previous versions have such vulnerabilities.	6.1	More Details
CVE-2023-6555	The Email Subscription Popup WordPress plugin before 1.2.20 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-6627	The WP Go Maps (formerly WP Google Maps) WordPress plugin before 9.0.28 does not properly protect most of its REST API routes, which attackers can abuse to store malicious HTML/Javascript on the site.	6.1	More Details
CVE-2023-50630	Cross Site Scripting (XSS) vulnerability in xiweicheng TMS v.2.28.0 allows a remote attacker to execute arbitrary code via a crafted script to the click here function.	6.1	More Details
CVE-2023-6981	The WP SMS – Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc plugin for WordPress is vulnerable to SQL Injection via the 'group_id' parameter in all versions up to, and including, 6.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This can leveraged to achieve Reflected Cross-site Scripting.	6.1	More Details
CVE-2024-21910	TinyMCE versions before 5.10.0 are affected by a cross-site scripting vulnerability. A remote and unauthenticated attacker could introduce crafted image or link URLs that would result in the execution of arbitrary JavaScript in an editing user's browser.	6.1	More Details
CVE-2024-21316	Windows Server Key Distribution Service Security Feature Bypass	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27000	Cross Site Scripting vulnerability found in NetScoutnGeniusOne v.6.3.4 allows a remote attacker to execute arbitrary code via the name parameter of the Profile and Exclusion List page(s).	6.1	More Details
CVE-2023-50092	APIIDA API Gateway Manager for Broadcom Layer7 v2023.2 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2023-38827	Cross Site Scripting vulnerability in Follet School Solutions Destiny v.20_0_1_AU4 and later allows a remote attacker to run arbitrary code via presentonesearchresultsform.do.	6.1	More Details
CVE-2023-52322	ecrire/public/assembler.php in SPIP before 4.1.13 and 4.2.x before 4.2.7 allows XSS because input from _request() is not restricted to safe characters such as alphanumerics.	6.1	More Details
CVE-2023-6629	The POST SMTP Mailer – Email log, Delivery Failure Notifications and Best Mail SMTP for WordPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘msg’ parameter in all versions up to, and including, 2.8.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-21908	TinyMCE versions before 5.9.0 are affected by a stored cross-site scripting vulnerability. An unauthenticated and remote attacker could insert crafted HTML into the editor resulting in arbitrary JavaScript execution in another user's browser.	6.1	More Details
CVE-2023-50093	APIIDA API Gateway Manager for Broadcom Layer7 v2023.2.2 is vulnerable to Host Header Injection.	6.1	More Details
CVE-2023-27739	easyXDM 2.5 allows XSS via the xdm_e parameter.	6.1	More Details
CVE-2023-50609	Cross Site Scripting (XSS) vulnerability in AVA teaching video application service platform version 3.1, allows remote attackers to execute arbitrary code via a crafted script to ajax.aspx.	6.1	More Details
CVE-2024-22075	Firefly III (aka firefly-iii) before 6.1.1 allows webhooks HTML Injection.	6.1	More Details
CVE-2023-6552	Lack of "current" GET parameter validation during the action of changing a language leads to an open redirect vulnerability.	6.1	More Details
CVE-2024-22048	govuk_tech_docs versions from 2.0.2 to before 3.3.1 are vulnerable to a cross-site scripting vulnerability. Malicious JavaScript may be executed in the user's browser if a malicious search result is displayed on the search page.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52197	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Impactpixel Ads Invalid Click Protection allows Stored XSS.This issue affects Ads Invalid Click Protection: from n/a through 1.0.	5.9	More Details
CVE-2023-52323	PyCryptodome and pycryptodomex before 3.19.1 allow side-channel leakage for OAEP decryption, exploitable for a Manger attack.	5.9	More Details
CVE-2024-21647	Puma is a web server for Ruby/Rack applications built for parallelism. Prior to version 6.4.2, puma exhibited incorrect behavior when parsing chunked transfer encoding bodies in a way that allowed HTTP request smuggling. Fixed versions limits the size of chunk extensions. Without this limit, an attacker could cause unbounded resource (CPU, network bandwidth) consumption. This vulnerability has been fixed in versions 6.4.2 and 5.6.8.	5.9	More Details
CVE-2023-52203	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Oliver Seidel, Bastian Germann cformsII allows Stored XSS.This issue affects cformsII: from n/a through 15.0.5.	5.9	More Details
CVE-2024-21306	Microsoft Bluetooth Driver Spoofing Vulnerability	5.7	More Details
CVE-2023-6944	A flaw was found in the Red Hat Developer Hub (RHDH). The catalog-import function leaks GitLab access tokens on the frontend when the base64 encoded GitLab token includes a newline at the end of the string. The sanitized error can display on the frontend, including the raw access token. Upon gaining access to this token and depending on permissions, an attacker could push malicious code to repositories, delete resources in Git, revoke or generate new keys, and sign code illegitimately.	5.7	More Details
CVE-2024-20692	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability	5.7	More Details
CVE-2023-50121	Autel EVO NANO drone flight control firmware version 1.6.5 is vulnerable to denial of service (DoS).	5.7	More Details
CVE-2023-6147	Qualys Jenkins Plugin for Policy Compliance prior to version and including 1.0.5 was identified to be affected by a security flaw, which was missing a permission check while performing a connectivity check to Qualys Cloud Services. This allowed any user with login access to configure or edit jobs to utilize the plugin and configure potential a rouge endpoint via which it was possible to control response for certain request which could be injected with XXE payloads leading to XXE while processing the response data	5.7	More Details
CVE-2023-6148	Qualys Jenkins Plugin for Policy Compliance prior to version and including 1.0.5 was identified to be affected by a security flaw, which was missing a permission check while performing a connectivity check to Qualys Cloud Services. This allowed any user with login access and access to configure or edit jobs to utilize the plugin to configure a potential rouge endpoint via which it was possible to control response for certain request which could be injected with XSS payloads leading to XSS while processing the response data	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6149	Qualys Jenkins Plugin for WAS prior to version and including 2.0.11 was identified to be affected by a security flaw, which was missing a permission check while performing a connectivity check to Qualys Cloud Services. This allowed any user with login access to configure or edit jobs to utilize the plugin and configure potential a rouge endpoint via which it was possible to control response for certain request which could be injected with XXE payloads leading to XXE while processing the response data	5.7	More Details
CVE-2023-7211	A vulnerability was found in Uniway Router 2.0. It has been declared as critical. This vulnerability affects unknown code of the component Administrative Web Interface. The manipulation leads to reliance on ip address for authentication. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. VDB-249766 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.6	More Details
CVE-2023-47559	A cross-site scripting (XSS) vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: QuMagie 2.2.1 and later	5.5	More Details
CVE-2023-46835	The current setup of the quarantine page tables assumes that the quarantine domain (dom_io) has been initialized with an address width of DEFAULT_DOMAIN_ADDRESS_WIDTH (48) and hence 4 page table levels. However dom_io being a PV domain gets the AMD-Vi IOMMU page tables levels based on the maximum (hot pluggable) RAM address, and hence on systems with no RAM above the 512GB mark only 3 page-table levels are configured in the IOMMU. On systems without RAM above the 512GB boundary amd_iommu_quarantine_init() will setup page tables for the scratch page with 4 levels, while the IOMMU will be configured to use 3 levels only, resulting in the last page table directory (PDE) effectively becoming a page table entry (PTE), and hence a device in quarantine mode gaining write access to the page destined to be a PDE. Due to this page table level mismatch, the sink page the device gets read/write access to is no longer cleared between device assignment, possibly leading to data leaks.	5.5	More Details
CVE-2023-36629	The ST ST54-android-packages-apps-Nfc package before 130-20230215-23W07p0 for Android has an out-of-bounds read.	5.5	More Details
CVE-2023-50974	In Appwrite CLI before 3.0.0, when using the login command, the credentials of the Appwrite user are stored in a ~/.appwrite/prefs.json file with 0644 as UNIX permissions. Any user of the local system can access those credentials.	5.5	More Details
CVE-2024-20694	Windows CoreMessaging Information Disclosure Vulnerability	5.5	More Details
CVE-2023-49555	An issue in YASM 1.3.0.86.g9def allows a remote attacker to cause a denial of service via the expand_smacro function in the modules/preprocs/nasm/nasm-pp.c component.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22368	The Spreadsheet::ParseXLSX package before 0.28 for Perl can encounter an out-of-memory condition during parsing of a crafted XLSX document. This occurs because the memoize implementation does not have appropriate constraints on merged cells.	5.5	More Details
CVE-2023-34328	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] AMD CPUs since ~2014 have extensions to normal x86 debugging functionality. Xen supports guests using these extensions. Unfortunately there are errors in Xen's handling of the guest state, leading to denials of service. 1) CVE-2023-34327 - An HVM vCPU can end up operating in the context of a previous vCPUs debug mask state. 2) CVE-2023-34328 - A PV vCPU can place a breakpoint over the live GDT. This allows the PV vCPU to exploit XSA-156 / CVE-2015-8104 and lock up the CPU entirely.	5.5	More Details
CVE-2023-34327	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] AMD CPUs since ~2014 have extensions to normal x86 debugging functionality. Xen supports guests using these extensions. Unfortunately there are errors in Xen's handling of the guest state, leading to denials of service. 1) CVE-2023-34327 - An HVM vCPU can end up operating in the context of a previous vCPUs debug mask state. 2) CVE-2023-34328 - A PV vCPU can place a breakpoint over the live GDT. This allows the PV vCPU to exploit XSA-156 / CVE-2015-8104 and lock up the CPU entirely.	5.5	More Details
CVE-2024-21311	Windows Cryptographic Services Information Disclosure Vulnerability	5.5	More Details
CVE-2023-34323	When a transaction is committed, C Xenstored will first check the quota is correct before attempting to commit any nodes. It would be possible that accounting is temporarily negative if a node has been removed outside of the transaction. Unfortunately, some versions of C Xenstored are assuming that the quota cannot be negative and are using assert() to confirm it. This will lead to C Xenstored crash when tools are built without -DNDEBUG (this is the default).	5.5	More Details
CVE-2023-49554	Use After Free vulnerability in YASM 1.3.0.86.g9def allows a remote attacker to cause a denial of service via the do_directive function in the modules/preprocs/nasm/nasm-pp.c component.	5.5	More Details
CVE-2024-20699	Windows Hyper-V Denial of Service Vulnerability	5.5	More Details
CVE-2023-49556	Buffer Overflow vulnerability in YASM 1.3.0.86.g9def allows a remote attacker to cause a denial of service via the expr_delete_term function in the libyasm/expr.c component.	5.5	More Details
CVE-2024-0344	A vulnerability, which was classified as critical, has been found in soxft TimeMail up to 1.1. Affected by this issue is some unknown functionality of the file check.php. The manipulation of the argument c leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250112.	5.5	More Details
CVE-2023-5091	Use After Free vulnerability in Arm Ltd Valhall GPU Kernel Driver allows a local non-privileged user to make improper GPU processing operations to gain access to already freed memory. This issue affects Valhall GPU Kernel Driver: from r37p0 through r40p0.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49557	An issue in YASM 1.3.0.86.g9def allows a remote attacker to cause a denial of service via the yasm_section_bcs_first function in the libyasm/section.c component.	5.5	More Details
CVE-2023-49558	An issue in YASM 1.3.0.86.g9def allows a remote attacker to cause a denial of service via the expand_mmac_params function in the modules/preprocs/nasm/nasm-pp.c component.	5.5	More Details
CVE-2023-6551	As a simple library, class.upload.php does not perform an in-depth check on uploaded files, allowing a stored XSS vulnerability when the default configuration is used. Developers must be aware of that fact and use extension whitelisting accompanied by forcing the server to always provide content-type based on the file extension. The README has been updated to include these guidelines.	5.4	More Details
CVE-2023-52149	Cross-Site Request Forgery (CSRF) vulnerability in Wow-Company Floating Button.This issue affects Floating Button: from n/a through 6.0.	5.4	More Details
CVE-2023-6798	The RSS Aggregator by Feedzy – Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to unauthorized settings update due to a missing capability check when updating settings in all versions up to, and including, 4.3.2. This makes it possible for authenticated attackers, with author-level access or above to change the plugin's settings including proxy settings, which are also exposed to authors.	5.4	More Details
CVE-2023-26998	Cross Site Scripting vulnerability found in NetScoutnGeniusOne v.6.3.4 allows a remote attacker to execute arbitrary code via the creator parameter of the Alert Configuration page.	5.4	More Details
CVE-2023-50136	Cross Site Scripting (XSS) vulnerability in JFinalcms 5.0.0 allows attackers to run arbitrary code via the name field when creating a new custom table.	5.4	More Details
CVE-2022-28975	A stored cross-site scripting (XSS) vulnerability in Infoblox NIOS v8.5.2-409296 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the VLAN View Name field.	5.4	More Details
CVE-2023-51246	A Cross Site Scripting (XSS) vulnerability in GetSimple CMS 3.3.16 exists when using Source Code Mode as a backend user to add articles via the /admin/edit.php page.	5.4	More Details
CVE-2023-41710	User-defined script code could be stored for a upsell related shop URL. This code was not correctly sanitized when adding it to DOM. Attackers could lure victims to user accounts with malicious script code and make them execute it in the context of a trusted domain. We added sanitization for this content. No publicly available exploits are known.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6788	The Metform Elementor Contact Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.8.1. This is due to missing or incorrect nonce validation on the contents function. This makes it possible for unauthenticated attackers to update the options "mf_hubsopt_token", "mf_hubsopt_refresh_token", "mf_hubsopt_token_type", and "mf_hubsopt_expires_in" via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This would allow an attacker to connect their own Hubspot account to a victim site's metform to obtain leads and contacts.	5.4	More Details
CVE-2023-6141	The Essential Real Estate WordPress plugin before 4.4.0 does not apply proper capability checks on its AJAX actions, which among other things, allow attackers with a subscriber account to conduct Stored XSS attacks.	5.4	More Details
CVE-2023-6738	The Page Builder: Pagelayer – Drag and Drop website builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pagelayer_header_code', 'pagelayer_body_open_code', and 'pagelayer_footer_code' meta fields in all versions up to, and including, 1.7.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This appears to be a reintroduction of a vulnerability patched in version 1.7.7.	5.4	More Details
CVE-2023-52120	Cross-Site Request Forgery (CSRF) vulnerability in Basix NEX-Forms – Ultimate Form Builder – Contact forms and much more.This issue affects NEX-Forms – Ultimate Form Builder – Contact forms and much more: from n/a through 8.5.2.	5.4	More Details
CVE-2023-52121	Cross-Site Request Forgery (CSRF) vulnerability in NitroPack Inc. NitroPack – Cache & Speed Optimization for Core Web Vitals, Defer CSS & JavaScript, Lazy load Images.This issue affects NitroPack – Cache & Speed Optimization for Core Web Vitals, Defer CSS & JavaScript, Lazy load Images: from n/a through 1.10.2.	5.4	More Details
CVE-2024-0201	The Product Expiry for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'save_settings' function in versions up to, and including, 2.5. This makes it possible for authenticated attackers, with subscriber-level permissions or above to update plugin settings.	5.4	More Details
CVE-2022-34344	Missing Authorization vulnerability in Rymera Web Co Wholesale Suite – WooCommerce Wholesale Prices, B2B, Catalog Mode, Order Form, Wholesale User Roles, Dynamic Pricing & More.This issue affects Wholesale Suite – WooCommerce Wholesale Prices, B2B, Catalog Mode, Order Form, Wholesale User Roles, Dynamic Pricing & More: from n/a through 2.1.5.	5.4	More Details
CVE-2023-29049	The "upsell" widget at the portal page could be abused to inject arbitrary script code. Attackers that manage to lure users to a compromised account, or gain temporary access to a legitimate account, could inject script code to gain persistent code execution capabilities under a trusted domain. User input for this widget is now sanitized to avoid malicious content the be processed. No publicly available exploits are known.	5.4	More Details
CVE-2023-50344	HCL DRYiCE MyXalytics is impacted by improper access control (Unauthenticated File Download) vulnerability. An unauthenticated user can download certain files.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21622	Craft is a content management system. This is a potential moderate impact, low complexity privilege escalation vulnerability in Craft starting in 3.x prior to 3.9.6 and 4.x prior to 4.4.16 with certain user permissions setups. This has been fixed in Craft 4.4.16 and Craft 3.9.6. Users should ensure they are running at least those versions.	5.4	More Details
CVE-2023-51673	Cross-Site Request Forgery (CSRF) vulnerability in Designful Stylish Price List – Price Table Builder & QR Code Restaurant Menu.This issue affects Stylish Price List – Price Table Builder & QR Code Restaurant Menu: from n/a through 7.0.17.	5.4	More Details
CVE-2023-29052	Users were able to define disclaimer texts for an upsell shop dialog that would contain script code that was not sanitized correctly. Attackers could lure victims to user accounts with malicious script code and make them execute it in the context of a trusted domain. We added sanitization for this content. No publicly available exploits are known.	5.4	More Details
CVE-2023-7223	A vulnerability classified as problematic has been found in Totolink T6 4.1.9cu.5241_B20210923. This affects an unknown part of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument topicurl with the input showSyslog leads to improper access controls. 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-249867. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2023-51408	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in StudioWombat WP Optin Wheel – Gamified Optin Email Marketing Tool for WordPress and WooCommerce.This issue affects WP Optin Wheel – Gamified Optin Email Marketing Tool for WordPress and WooCommerce: from n/a through 1.4.3.	5.3	More Details
CVE-2023-5770	Proofpoint Enterprise Protection contains a vulnerability in the email delivery agent that allows an unauthenticated attacker to inject improperly encoded HTML into the email body of a message through the email subject. The vulnerability is caused by inappropriate encoding when rewriting the email before delivery.This issue affects Proofpoint Enterprise Protection: from 8.20.2 before patch 4809, from 8.20.0 before patch 4805, from 8.18.6 before patch 4804 and all other prior versions.	5.3	More Details
CVE-2023-52208	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Constant Contact Constant Contact Forms.This issue affects Constant Contact Forms: from n/a through 2.4.2.	5.3	More Details
CVE-2023-52146	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Aaron J 404 Solution.This issue affects 404 Solution: from n/a through 2.33.0.	5.3	More Details
CVE-2023-52148	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in wp.Insider, wpaffiliatemgr Affiliates Manager.This issue affects Affiliates Manager: from n/a through 2.9.30.	5.3	More Details
CVE-2023-52126	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Suman Bhattarai Send Users Email.This issue affects Send Users Email: from n/a through 1.4.3.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22049	httparty before 0.21.0 is vulnerable to an assumed-immutable web parameter vulnerability. A remote and unauthenticated attacker can provide a crafted filename parameter during multipart/form-data uploads which could result in attacker controlled filenames being written.	5.3	More Details
CVE-2023-52151	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Uncanny Automator, Uncanny Owl Uncanny Automator – Automate everything with the #1 no-code automation and integration plugin.This issue affects Uncanny Automator – Automate everything with the #1 no-code automation and integration plugin: from n/a through 5.1.0.2.	5.3	More Details
CVE-2022-2586	It was discovered that a nft object or expression could reference a nft set on a different nft table, leading to a use-after-free once that table was deleted.	5.3	More Details
CVE-2023-51508	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Jordy Meow Database Cleaner: Clean, Optimize & Repair.This issue affects Database Cleaner: Clean, Optimize & Repair: from n/a through 0.9.8.	5.3	More Details
CVE-2024-21313	Windows TCP/IP Information Disclosure Vulnerability	5.3	More Details
CVE-2022-45354	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in WPChill Download Monitor.This issue affects Download Monitor: from n/a through 4.7.60.	5.3	More Details
CVE-2023-51701	fastify-reply-from is a Fastify plugin to forward the current HTTP request to another server. A reverse proxy server built with `@fastify/reply-from` could misinterpret the incoming body by passing an header `ContentType: application/json ; charset=utf-8`. This can lead to bypass of security checks. This vulnerability has been patched in '@fastify/reply-from` version 9.6.0.	5.3	More Details
CVE-2024-21645	pyLoad is the free and open-source Download Manager written in pure Python. A log injection vulnerability was identified in `pyload` allowing any unauthenticated actor to inject arbitrary messages into the logs gathered by `pyload`. Forged or otherwise, corrupted log files can be used to cover an attacker’s tracks or even to implicate another party in the commission of a malicious act. This vulnerability has been patched in version 0.5.0b3.dev77.	5.3	More Details
CVE-2024-0305	A vulnerability was found in Guangzhou Yingke Electronic Technology Ncast up to 2017 and classified as problematic. Affected by this issue is some unknown functionality of the file /manage/IPSetup.php of the component Guest Login. The manipulation leads to information disclosure. 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-249872.	5.3	More Details
CVE-2022-2585	It was discovered that when exec'ing from a non-leader thread, armed POSIX CPU timers would be left on a list but freed, leading to a use-after-free.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6984	The PowerPack Addons for Elementor (Free Widgets, Extensions and Templates) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.7.13. This is due to missing or incorrect nonce validation in the powerpack-lite-for-elementor/classes/class-pp-admin-settings.php file. This makes it possible for unauthenticated attackers to modify and reset plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.3	More Details
CVE-2023-51406	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ninja Team FastDup – Fastest WordPress Migration & Duplicator.This issue affects FastDup – Fastest WordPress Migration & Duplicator: from n/a through 2.1.7.	5.3	More Details
CVE-2022-2588	It was discovered that the cls_route filter implementation in the Linux kernel would not remove an old filter from the hashtable before freeing it if its handle had the value 0.	5.3	More Details
CVE-2024-0263	A vulnerability was found in ACME Ultra Mini HTTPd 1.21. It has been classified as problematic. This affects an unknown part of the component HTTP GET Request Handler. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-249819.	5.3	More Details
CVE-2024-0261	A vulnerability has been found in Sentex FTPDMIN 0.96 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component RNFR Command Handler. The manipulation leads to denial of service. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-249817 was assigned to this vulnerability.	5.3	More Details
CVE-2023-51490	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in WPMU DEV Defender Security – Malware Scanner, Login Security & Firewall.This issue affects Defender Security – Malware Scanner, Login Security & Firewall: from n/a through 4.1.0.	5.3	More Details
CVE-2022-2602	io_uring UAF, Unix SCM garbage collection	5.3	More Details
CVE-2023-46906	juzaweb <= 3.4 is vulnerable to Incorrect Access Control, resulting in an application outage after a 500 HTTP status code. The payload in the timezone field was not correctly validated.	4.9	More Details
CVE-2023-34324	Closing of an event channel in the Linux kernel can result in a deadlock. This happens when the close is being performed in parallel to an unrelated Xen console action and the handling of a Xen console interrupt in an unprivileged guest. The closing of an event channel is e.g. triggered by removal of a paravirtual device on the other side. As this action will cause console messages to be issued on the other side quite often, the chance of triggering the deadlock is not neglectable. Note that 32-bit Arm-guests are not affected, as the 32-bit Linux kernel on Arm doesn't use queued-RW-locks, which are required to trigger the issue (on Arm32 a waiting writer doesn't block further readers to get the lock).	4.9	More Details
CVE-2024-20662	Windows Online Certificate Status Protocol (OCSP) Information Disclosure Vulnerability	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3726	OCSInventory allow stored email template with special characters that lead to a Stored cross-site Scripting.	4.9	More Details
CVE-2024-0226	Synopsys Seeker versions prior to 2023.12.0 are vulnerable to a stored cross-site scripting vulnerability through a specially crafted payload.	4.8	More Details
CVE-2023-46741	CubeFS is an open-source cloud-native file storage system. A vulnerability was found in CubeFS prior to version 3.3.1 that could allow users to read sensitive data from the logs which could allow them escalate privileges. CubeFS leaks configuration keys in plaintext format in the logs. These keys could allow anyone to carry out operations on blobs that they otherwise do not have permissions for. For example, an attacker that has succesfully retrieved a secret key from the logs can delete blogs from the blob store. The attacker can either be an internal user with limited privileges to read the log, or they can be an external user who has escalated privileges sufficiently to access the logs. The vulnerability has been patched in v3.3.1. There is no other mitigation than upgrading.	4.8	More Details
CVE-2023-5911	The WP Custom Cursors	WordPress Cursor Plugin WordPress plugin through 3.2 does not sanitise 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-2023-46742	CubeFS is an open-source cloud-native file storage system. CubeFS prior to version 3.3.1 was found to leak users secret keys and access keys in the logs in multiple components. When CubeCS creates new users, it leaks the users secret key. This could allow a lower-privileged user with access to the logs to retrieve sensitive information and impersonate other users with higher privileges than themselves. The issue has been patched in v3.3.1. There is no other mitigation than upgrading CubeFS.	4.8	More Details
CVE-2023-6004	A flaw was found in libssh. By utilizing the ProxyCommand or ProxyJump feature, users can exploit unchecked hostname syntax on the client. This issue may allow an attacker to inject malicious code into the command of the features mentioned through the hostname parameter.	4.8	More Details
CVE-2023-38678	OOB access in paddle.mode in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service.	4.7	More Details
CVE-2023-52312	Nullptr dereference in paddle.crop in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service.	4.7	More Details
CVE-2023-52308	FPE in paddle.amin in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service.	4.7	More Details
CVE-2023-52306	FPE in paddle.lerp in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52305	FPE in paddle.topk in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service.	4.7	More Details
CVE-2023-52303	Nullptr in paddle.put_along_axis in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service.	4.7	More Details
CVE-2023-52302	Nullptr in paddle.nextafter in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service.	4.7	More Details
CVE-2023-38677	FPE in paddle.linalg.eig in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service.	4.7	More Details
CVE-2023-46836	The fixes for XSA-422 (Branch Type Confusion) and XSA-434 (Speculative Return Stack Overflow) are not IRQ-safe. It was believed that the mitigations always operated in contexts with IRQs disabled. However, the original XSA-254 fix for Meltdown (XPTI) deliberately left interrupts enabled on two entry paths; one unconditionally, and one conditionally on whether XPTI was active. As BTC/SRSO and Meltdown affect different CPU vendors, the mitigations are not active together by default. Therefore, there is a race condition whereby a malicious PV guest can bypass BTC/SRSO protections and launch a BTC/SRSO attack against Xen.	4.7	More Details
CVE-2023-38676	Nullptr in paddle.dot in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service.	4.7	More Details
CVE-2023-38675	FPE in paddle.linalg.matrix_rank in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service.	4.7	More Details
CVE-2023-38674	FPE in paddle.nanmedian in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service.	4.7	More Details
CVE-2023-1032	The Linux kernel io_uring IORING_OP_SOCKET operation contained a double free in function __sys_socket_file() in file net/socket.c. This issue was introduced in da214a475f8bd1d3e9e7a19ddfeb4d1617551bab and fixed in 649c15c7691e9b13cbe9bf6c65c365350e056067.	4.7	More Details
CVE-2023-7212	A vulnerability classified as critical has been found in DeDeCMS up to 5.7.112. Affected is an unknown function of the file file_class.php of the component Backend. 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. The identifier of this vulnerability is VDB-249768. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2023-52313	FPE in paddle.argmin and paddle.argmax in PaddlePaddle before 2.6.0. This flaw can cause a runtime crash and a denial of service.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20691	Windows Themes Information Disclosure Vulnerability	4.7	More Details
CVE-2024-22370	In JetBrains YouTrack before 2023.3.22666 stored XSS via markdown was possible	4.6	More Details
CVE-2024-20802	Improper access control vulnerability in Samsung DeX prior to SMR Jan-2024 Release 1 allows owner to access other users' notification in a multi-user environment.	4.6	More Details
CVE-2022-3864	A vulnerability exists in the Relion update package signature validation. A tampered update package could cause the IED to restart. After restart the device is back to normal operation. An attacker could exploit the vulnerability by first gaining access to the system with security privileges and attempt to update the IED with a malicious update package. Successful exploitation of this vulnerability will cause the IED to restart, causing a temporary Denial of Service.	4.5	More Details
CVE-2024-0340	A vulnerability was found in vhost_new_msg in drivers/vhost/vhost.c in the Linux kernel, which does not properly initialize memory in messages passed between virtual guests and the host operating system in the vhost/vhost.c:vhost_new_msg() function. This issue can allow local privileged users to read some kernel memory contents when reading from the /dev/vhost-net device file.	4.4	More Details
CVE-2023-6842	The Formidable Forms – Contact Form, Survey, Quiz, Payment, Calculator Form & Custom Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the name field label and description field label parameter in all versions up to 6.7 (inclusive) due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, this only affects multi-site installations and installations where unfiltered_html has been disabled. However, in the formidable settings admins can extend form creation, deletion and other management permissions to other user types, which makes it possible for this vulnerability to be exploited by lower level user types as long as they have been granted the proper permissions.	4.4	More Details
CVE-2024-21305	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability	4.4	More Details
CVE-2024-21668	react-native-mmkv is a library that allows easy use of MMKV inside React Native applications. Before version 2.11.0, the react-native-mmkv logged the optional encryption key for the MMKV database into the Android system log. The key can be obtained by anyone with access to the Android Debugging Bridge (ADB) if it is enabled in the phone settings. This bug is not present on iOS devices. By logging the encryption secret to the system logs, attackers can trivially recover the secret by enabling ADB and undermining an app's thread model. This issue has been patched in version 2.11.0.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6498	The Complianz – GDPR/CCPA Cookie Consent plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to and including 6.5.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2023-6594	The WordPress Button Plugin MaxButtons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 9.7.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. Administrators can give button creation privileges to users with lower levels (contributor+) which would allow those lower-privileged users to carry out attacks.	4.4	More Details
CVE-2023-41779	There is an illegal memory access vulnerability of ZTE's ZXCLOUD iRAI product.When the vulnerability is exploited by an attacker with the common user permission, the physical machine will be crashed.	4.4	More Details
CVE-2023-41783	There is a command injection vulnerability of ZTE's ZXCLOUD iRAI. Due to the program failed to adequately validate the user's input, an attacker could exploit this vulnerability to escalate local privileges.	4.3	More Details
CVE-2023-52128	Cross-Site Request Forgery (CSRF) vulnerability in WhiteWP White Label – WordPress Custom Admin, Custom Login Page, and Custom Dashboard.This issue affects White Label – WordPress Custom Admin, Custom Login Page, and Custom Dashboard: from n/a through 2.9.0.	4.3	More Details
CVE-2023-51535	Cross-Site Request Forgery (CSRF) vulnerability in CleanTalk - Anti-Spam Protection Spam protection, Anti-Spam, FireWall by CleanTalk.This issue affects Spam protection, Anti-Spam, FireWall by CleanTalk: from n/a through 6.20.	4.3	More Details
CVE-2023-52145	Cross-Site Request Forgery (CSRF) vulnerability in Marios Alexandrou Republish Old Posts.This issue affects Republish Old Posts: from n/a through 1.21.	4.3	More Details
CVE-2024-0286	A vulnerability, which was classified as problematic, was found in PHPGurukul Hospital Management System 1.0. This affects an unknown part of the file index.php#contact_us of the component Contact Form. The manipulation of the argument Name/Email/Message 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-249843.	4.3	More Details
CVE-2023-6980	The WP SMS – Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.5. This is due to missing or incorrect nonce validation on the 'delete' action of the wp-sms-subscribers page. This makes it possible for unauthenticated attackers to delete subscribers 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 Number	Description	Base Score	Reference
CVE-2023-52222	Cross-Site Request Forgery (CSRF) vulnerability in Automattic WooCommerce.This issue affects WooCommerce: from n/a through 8.2.2.	4.3	More Details
CVE-2023-52136	Cross-Site Request Forgery (CSRF) vulnerability in Smash Balloon Custom Twitter Feeds – A Tweets Widget or X Feed Widget.This issue affects Custom Twitter Feeds – A Tweets Widget or X Feed Widget: from n/a through 2.1.2.	4.3	More Details
CVE-2023-52130	Cross-Site Request Forgery (CSRF) vulnerability in wp.Insider, wpaffiliatemgr Affiliates Manager.This issue affects Affiliates Manager: from n/a through 2.9.31.	4.3	More Details
CVE-2023-52127	Cross-Site Request Forgery (CSRF) vulnerability in WPClever WPC Product Bundles for WooCommerce.This issue affects WPC Product Bundles for WooCommerce: from n/a through 7.3.1.	4.3	More Details
CVE-2024-0348	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been classified as problematic. Affected is an unknown function of the component File Upload Handler. The manipulation leads to resource consumption. 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-250116.	4.3	More Details
CVE-2023-52123	Cross-Site Request Forgery (CSRF) vulnerability in WPChill Strong Testimonials.This issue affects Strong Testimonials: from n/a through 3.1.10.	4.3	More Details
CVE-2023-52184	Cross-Site Request Forgery (CSRF) vulnerability in WP Job Portal WP Job Portal – A Complete Job Board.This issue affects WP Job Portal – A Complete Job Board: from n/a through 2.0.6.	4.3	More Details
CVE-2023-52216	Cross-Site Request Forgery (CSRF) vulnerability in Yevhen Kotelnytskyi JS & CSS Script Optimizer.This issue affects JS & CSS Script Optimizer: from n/a through 0.3.3.	4.3	More Details
CVE-2024-0266	A vulnerability classified as problematic has been found in Project Worlds Online Lawyer Management System 1.0. Affected is an unknown function of the component User Registration. The manipulation of the argument First Name 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-249822 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2024-0246	A vulnerability classified as problematic has been found in IceWarp 12.0.2.1/12.0.3.1. This affects an unknown part of the file /install/ of the component Utility Download Handler. The manipulation of the argument lang with the input 1%27"()%26%25<zzz><ScRiPt>alert(document.domain)</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-249759. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6493	The Depicter Slider – Responsive Image Slider, Video Slider & Post Slider plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.6. This is due to missing or incorrect nonce validation on the 'save' function. This makes it possible for unauthenticated attackers to modify the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. CVE-2023-51491 appears to be a duplicate of this issue.	4.3	More Details
CVE-2024-0343	A vulnerability classified as problematic was found in CodeAstro Simple House Rental System 5.6. Affected by this vulnerability is an unknown functionality of the component Login Panel. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250111.	4.3	More Details
CVE-2024-21664	jwx is a Go module implementing various JWx (JWA/JWE/JWK/JWS/JWT, otherwise known as JOSE) technologies. Calling `jws.Parse` with a JSON serialized payload where the `signature` field is present while `protected` is absent can lead to a nil pointer dereference. The vulnerability can be used to crash/DOS a system doing JWS verification. This vulnerability has been patched in versions 2.0.19 and 1.2.28.	4.3	More Details
CVE-2024-0345	A vulnerability, which was classified as problematic, was found in CodeAstro Vehicle Booking System 1.0. This affects an unknown part of the file usr/usr-register.php of the component User Registration. The manipulation of the argument Full_Name/Last_Name/Address with the input <script>alert(document.cookie)</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 identifier VDB-250113 was assigned to this vulnerability.	4.3	More Details
CVE-2023-51678	Cross-Site Request Forgery (CSRF) vulnerability in Doofinder Doofinder WP & WooCommerce Search.This issue affects Doofinder WP & WooCommerce Search: from n/a through 2.0.33.	4.3	More Details
CVE-2023-41287	A SQL injection vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow users to inject malicious code via a network. We have already fixed the vulnerability in the following version: Video Station 5.7.2 (2023/11/23) and later	4.3	More Details
CVE-2023-52119	Cross-Site Request Forgery (CSRF) vulnerability in Icegram Icegram Engage – WordPress Lead Generation, Popup Builder, CTA, Optins and Email List Building.This issue affects Icegram Engage – WordPress Lead Generation, Popup Builder, CTA, Optins and Email List Building: from n/a through 3.1.18.	4.3	More Details
CVE-2023-7068	The WooCommerce PDF Invoices, Packing Slips, Delivery Notes and Shipping Labels plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on theprint_packinglist action in all versions up to, and including, 4.3.0. This makes it possible for authenticated attackers, with subscriber-level access and above, to export orders which can contain sensitive information.	4.3	More Details
CVE-2024-0260	A vulnerability, which was classified as problematic, was found in SourceCodester Engineers Online Portal 1.0. Affected is an unknown function of the file change_password_teacher.php of the component Password Change. The manipulation leads to session expiration. 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-249816.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51538	Cross-Site Request Forgery (CSRF) vulnerability in Awesome Support Team Awesome Support – WordPress HelpDesk & Support Plugin.This issue affects Awesome Support – WordPress HelpDesk & Support Plugin: from n/a through 6.1.5.	4.3	More Details
CVE-2023-51668	Cross-Site Request Forgery (CSRF) vulnerability in WP Zone Inline Image Upload for BBPress.This issue affects Inline Image Upload for BBPress: from n/a through 1.1.18.	4.3	More Details
CVE-2023-51539	Cross-Site Request Forgery (CSRF) vulnerability in Apollo13Themes Apollo13 Framework Extensions.This issue affects Apollo13 Framework Extensions: from n/a through 1.9.1.	4.3	More Details
CVE-2024-22164	In Splunk Enterprise Security (ES) versions below 7.1.2, an attacker can use investigation attachments to perform a denial of service (DoS) to the Investigation. The attachment endpoint does not properly limit the size of the request which lets an attacker cause the Investigation to become inaccessible.	4.3	More Details
CVE-2023-52122	Cross-Site Request Forgery (CSRF) vulnerability in PressTigers Simple Job Board.This issue affects Simple Job Board: from n/a through 2.10.6.	4.3	More Details
CVE-2024-22124	Under certain conditions, Internet Communication Manager (ICM) or SAP Web Dispatcher - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22_EXT, WEBDISP 7.22_EXT, WEBDISP 7.53, WEBDISP 7.54, could allow an attacker to access information which would otherwise be restricted causing high impact on confidentiality.	4.1	More Details
CVE-2024-21738	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation.	4.1	More Details
CVE-2024-20804	Path traversal vulnerability in FileUriConverter of MyFiles prior to SMR Jan-2024 Release 1 in Android 11 and Android 12, and version 14.5.00.21 in Android 13 allows local attackers to write arbitrary file.	4.0	More Details
CVE-2024-20809	Improper access control vulnerability in Nearby device scanning prior version 11.1.14.7 allows local attacker to access data.	4.0	More Details
CVE-2023-6992	Cloudflare version of zlib library was found to be vulnerable to memory corruption issues affecting the deflation algorithm implementation (deflate.c). The issues resulted from improper input validation and heap-based buffer overflow. A local attacker could exploit the problem during compression using a crafted malicious file potentially leading to denial of service of the software. Patches: The issue has been patched in commit 8352d10 https://github.com/cloudflare/zlib/commit/8352d108c05db1bdc5ac3bdf834dad641694c13c . The upstream repository is not affected.	4.0	More Details
CVE-2023-47140	IBM CICS Transaction Gateway 9.3 could allow a user to transfer or view files due to improper access controls.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20808	Improper access control vulnerability in Nearby device scanning prior version 11.1.14.7 allows local attacker to access data.	4.0	More Details
CVE-2023-41782	There is a DLL hijacking vulnerability in ZTE ZXCLOUD iRAI, an attacker could place a fake DLL file in a specific directory and successfully exploit this vulnerability to execute malicious code.	3.9	More Details
CVE-2023-45043	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	3.8	More Details
CVE-2023-45041	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	3.8	More Details
CVE-2023-45042	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	3.8	More Details
CVE-2023-45040	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	3.8	More Details
CVE-2023-45039	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	3.8	More Details
CVE-2023-45044	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	3.8	More Details
CVE-2024-0349	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to sensitive cookie without secure attribute. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-250117 was assigned to this vulnerability.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21734	SAP Marketing (Contacts App) - version 160, allows an attacker with low privileges to trick a user to open malicious page which could lead to a very convincing phishing attack with low impact on confidentiality and integrity of the application.	3.7	More Details
CVE-2023-50345	HCL DRYiCE MyXalytics is impacted by an Open Redirect vulnerability which could allow an attacker to redirect users to malicious sites, potentially leading to phishing attacks or other security threats.	3.7	More Details
CVE-2024-0347	A vulnerability was found in SourceCodester Engineers Online Portal 1.0 and classified as problematic. This issue affects some unknown processing of the file signup_teacher.php. The manipulation of the argument Password leads to weak password requirements. 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-250115.	3.7	More Details
CVE-2022-40696	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in WP Engine Advanced Custom Fields (ACF).This issue affects Advanced Custom Fields (ACF): from 3.1.1 through 6.0.2.	3.7	More Details
CVE-2023-47219	A SQL injection vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: QuMagie 2.2.1 and later	3.5	More Details
CVE-2023-7215	A vulnerability, which was classified as problematic, has been found in Chanzhaoyu chatgpt-web 2.11.1. This issue affects some unknown processing. The manipulation of the argument Description with the input <image src onerror=prompt(document.domain)> 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-249779.	3.5	More Details
CVE-2024-0341	A vulnerability was found in Inis up to 2.0.1. It has been rated as problematic. This issue affects some unknown processing of the file /app/api/controller/default/File.php of the component GET Request Handler. The manipulation of the argument path leads to path traversal: '../filedir'. The exploit has been disclosed to the public and may be used. The identifier VDB-250109 was assigned to this vulnerability.	3.5	More Details
CVE-2024-0282	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been classified as problematic. This affects an unknown part of the file addmaterialsubmit.php. The manipulation of the argument tin 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 identifier VDB-249837 was assigned to this vulnerability.	3.5	More Details
CVE-2024-0284	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been rated as problematic. This issue affects some unknown processing of the file party_submit.php. The manipulation of the argument party_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-249839.	3.5	More Details
CVE-2024-0283	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file party_details.php. The manipulation of the argument party_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-249838 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0346	A vulnerability has been found in CodeAstro Vehicle Booking System 1.0 and classified as problematic. This vulnerability affects unknown code of the file usr/user-give-feedback.php of the component Feedback Page. The manipulation of the argument My Testemonial leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-250114 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-20805	Path traversal vulnerability in ZipCompressor of MyFiles prior to SMR Jan-2024 Release 1 in Android 11 and Android 12, and version 14.5.00.21 in Android 13 allows local attackers to write arbitrary file.	3.3	More Details
CVE-2023-51744	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted CGM files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	3.3	More Details
CVE-2024-0217	A use-after-free flaw was found in PackageKitd. In some conditions, the order of cleanup mechanics for a transaction could be impacted. As a result, some memory access could occur on memory regions that were previously freed. Once freed, a memory region can be reused for other allocations and any previously stored data in this memory region is considered lost.	3.3	More Details
CVE-2024-20807	Implicit intent hijacking vulnerability in Samsung Email prior to version 6.1.90.16 allows local attacker to get sensitive information.	3.3	More Details
CVE-2023-34321	Arm provides multiple helpers to clean & invalidate the cache for a given region. This is, for instance, used when allocating guest memory to ensure any writes (such as the ones during scrubbing) have reached memory before handing over the page to a guest. Unfortunately, the arithmetics in the helpers can overflow and would then result to skip the cache cleaning/invalidation. Therefore there is no guarantee when all the writes will reach the memory.	3.3	More Details
CVE-2023-46837	Arm provides multiple helpers to clean & invalidate the cache for a given region. This is, for instance, used when allocating guest memory to ensure any writes (such as the ones during scrubbing) have reached memory before handing over the page to a guest. Unfortunately, the arithmetics in the helpers can overflow and would then result to skip the cache cleaning/invalidation. Therefore there is no guarantee when all the writes will reach the memory. This undefined behavior was meant to be addressed by XSA-437, but the approach was not sufficient.	3.3	More Details
CVE-2024-22047	A race condition exists in Audited 4.0.0 to 5.3.3 that can result in an authenticated user to cause audit log entries to be attributed to another user.	3.1	More Details
CVE-2023-50346	HCL DRYiCE MyXalytics is impacted by an information disclosure vulnerability. Certain endpoints within the application disclose detailed file information.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50348	HCL DRYiCE MyXalytics is impacted by an improper error handling vulnerability. The application returns detailed error messages that can provide an attacker with insight into the application, system, etc.	3.1	More Details
CVE-2024-0350	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to session expiration. The attack may be launched 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. VDB-250118 is the identifier assigned to this vulnerability.	3.1	More Details
CVE-2024-0351	A vulnerability classified as problematic has been found in SourceCodester Engineers Online Portal 1.0. This affects an unknown part. The manipulation leads to session fixiation. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250119.	3.1	More Details
CVE-2024-0262	A vulnerability was found in Online Job Portal 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /Admin/News.php of the component Create News Page. The manipulation of the argument News with the input </title> <scRipt>alert(0x00C57D)</scRipt> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-249818 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2022-43375	Rejected reason: This CVE ID was unused by the CNA.	N/A	More Details
CVE-2022-29409	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-52141	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2023. Notes: none.	N/A	More Details
CVE-2023-52140	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2023. Notes: none.	N/A	More Details
CVE-2023-5442	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-6991. Reason: This candidate is a reservation duplicate of CVE-2023-6991. Notes: All CVE users should reference CVE-2023-43226 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-5619	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-6530. Reason: This candidate is a reservation duplicate of CVE-2023-6530. Notes: All CVE users should reference CVE-2023-43226 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0228	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is a duplicate of CVE-2024-0193.	N/A	More Details