SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 15 May 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-2024-32700	Unrestricted Upload of File with Dangerous Type vulnerability in Kognetiks Kognetiks Chatbot for WordPress.This issue affects Kognetiks Chatbot for WordPress: from n/a through 2.0.0.	10.0	More Details
CVE-2024-30207	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). The affected systems use symmetric cryptography with a hard-coded key to protect the communication between client and server. This could allow an unauthenticated remote attacker to compromise confidentiality and integrity of the communication and, subsequently, availability of the system. A successful exploit requires the attacker to gain knowledge of the hard-coded key and to be able to intercept the communication between client and server on the network.	10.0	More Details
CVE-2024-31377	Unrestricted Upload of File with Dangerous Type vulnerability in J.N. Breetvelt a.K.A. OpaJaap WP Photo Album Plus.This issue affects WP Photo Album Plus: from n/a through 8.7.01.001.	10.0	More Details
CVE-2024-32741	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V3.0). The affected device contains hard coded password which is used for the privileged system user `root` and for the boot loader `GRUB` by default . An attacker who manages to crack the password hash gains root access to the device.	10.0	More Details
CVE-2024-29895	Cacti provides an operational monitoring and fault management framework. A command injection vulnerability on the 1.3.x DEV branch allows any unauthenticated user to execute arbitrary command on the server when `register_argc_argv` option of PHP is `On`. In `cmd_realtime.php` line 119, the `$poller_id` used as part of the command execution is sourced from `$_SERVER['argv']`, which can be controlled by URL when `register_argc_argv` option of PHP is `On`. And this option is `On` by default in many environments such as the main PHP Docker image for PHP. Commit 53e8014d1f082034e0646edc6286cde3800c683d contains a patch for the issue, but this commit was reverted in commit 99633903cad0de5ace636249de16f77e57a3c8fc.	10.0	More Details
CVE-2024-34411	Unrestricted Upload of File with Dangerous Type vulnerability in Thomas Scholl canvasio3D Light.This issue affects canvasio3D Light: from n/a through 2.5.0.	9.9	More Details
CVE-2024-4701	A path traversal issue potentially leading to remote code execution in Genie for all versions prior to 4.3.18	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4393	The Social Connect plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.2. This is due to insufficient verification on the OpenID server being supplied during the social login through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email.	9.8	More Details
CVE-2024-3070	The Last Viewed Posts by WPBeginner plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.0.0 via deserialization of untrusted input from the LastViewedPosts Cookie. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	9.8	More Details
CVE-2024-4434	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to time-based SQL Injection via the ‘term_id’ parameter in versions up to, and including, 4.2.6.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.8	More Details
CVE-2024-4413	The Hotel Booking Lite plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 4.11.1 via deserialization of untrusted input. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	9.8	More Details
CVE-2024-3806	The Porto theme for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 7.1.0 via the 'porto_ajax_posts' function. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where php file type can be uploaded and included.	9.8	More Details
CVE-2024-3263	YMS VIS Pro is an information system for veterinary and food administration, veterinarians and farm. Due to a combination of improper method for system credentials generation and weak password policy, passwords can be easily guessed and enumerated through brute force attacks. Successful attacks can lead to unauthorised access and execution of operations based on assigned user permissions. This vulnerability affects VIS Pro in versions <= 3.3.0.6. This vulnerability has been mitigated by changes in authentication mechanisms and implementation of additional authentication layer and strong password policies.	9.8	More Details
CVE-2024-34945	Tenda FH1206 V1.2.0.8(8155)_EN was discovered to contain a stack-based buffer overflow vulnerability via the PPW parameter at ip/goform/WizardHandle.	9.8	More Details
CVE-2024-35099	TOTOLINK LR350 V9.3.5u.6698_B20230810 was discovered to contain a stack overflow via the password parameter in the function loginAuth.	9.8	More Details
CVE-2024-34943	Tenda FH1206 V1.2.0.8(8155)_EN was discovered to contain a stack-based buffer overflow vulnerability via the page parameter at ip/goform/NatStaticSetting.	9.8	More Details
CVE-2024-34706	Valtimo is an open source business process and case management platform. When opening a form in Valtimo, the access token (JWT) of the user is exposed to `api.form.io` via the the `x-jwt-token` header. An attacker can retrieve personal information from this token, or use it to execute requests to the Valtimo REST API on behalf of the logged-in user. This issue is caused by a misconfiguration of the Form.io component. The following conditions have to be met in order to perform this attack: An attacker needs to have access to the network traffic on the `api.form.io` domain; the content of the `x-jwt-token` header is logged or otherwise available to the attacker; an attacker needs to have network access to the Valtimo API; and an attacker needs to act within the time-to-live of the access token. The default TTL in Keycloak is 5 minutes. Versions 10.8.4, 11.1.6 and 11.2.2 have been patched.	9.8	More Details
CVE-2024-25517	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the tbTable argument at /WebUtility/MF.aspx.	9.8	More Details
CVE-2024-34213	TOTOLINK CP450 v4.1.0cu.747_B20191224 was discovered to contain a stack buffer overflow vulnerability in the SetPortForwardRules function.	9.8	More Details
CVE-2024-34209	TOTOLINK CP450 v4.1.0cu.747_B20191224 was discovered to contain a stack buffer overflow vulnerability in the setIpPortFilterRules function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4560	The Kognetiks Chatbot for WordPress plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the chatbot_chatgpt_upload_file_to_assistant function in all versions up to, and including, 1.9.9. This makes it possible for unauthenticated attackers, with to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2024-4825	A vulnerability has been discovered in Agentejo Cockpit CMS v0.5.5 that consists in an arbitrary file upload in '/media/api' parameter via post request. An attacker could upload files to the server, compromising the entire infrastructure.	9.8	More Details
CVE-2024-4824	Vulnerability in School ERP Pro+Responsive 1.0 that allows SQL injection through the '/SchoolERP/office_admin/' index in the parameters groups_id, examname, classes_id, es_voucherid, es_class, etc. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the database.	9.8	More Details
CVE-2024-4778	Memory safety bugs present in Firefox 125. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 126.	9.8	More Details
CVE-2024-31472	There are command injection vulnerabilities in the underlying Soft AP Daemon service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2024-31471	There is a command injection vulnerability in the underlying Central Communications service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2024-31470	There is a buffer overflow vulnerability in the underlying SAE (Simultaneous Authentication of Equals) service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2024-31469	There are buffer overflow vulnerabilities in the underlying Central Communications service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2024-31468	There are buffer overflow vulnerabilities in the underlying Central Communications service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2024-31467	There are buffer overflow vulnerabilities in the underlying CLI service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2024-31466	There are buffer overflow vulnerabilities in the underlying CLI service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2024-4764	Multiple WebRTC threads could have claimed a newly connected audio input leading to use-after-free. This vulnerability affects Firefox < 126.	9.8	More Details
CVE-2024-33874	HDF5 Library through 1.14.3 has a heap buffer overflow in H5O__mtime_new_encode in H5Omtime.c.	9.8	More Details
CVE-2024-33485	SQL Injection vulnerability in CASAP Automated Enrollment System using PHP/MySQLi with Source Code V1.0 allows a remote attacker to obtain sensitive information via a crafted payload to the login.php component	9.8	More Details
CVE-2024-34256	OFCMS V1.1.2 is vulnerable to SQL Injection via the new table function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33868	An issue was discovered in linqi before 1.4.0.1 on Windows. There is LDAP injection.	9.8	More Details
CVE-2024-33863	An issue was discovered in linqi before 1.4.0.1 on Windows. There is /api/Cdn/GetFile local file inclusion.	9.8	More Details
CVE-2024-32740	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V3.0). The affected device contains undocumented users and credentials. An attacker could misuse the credentials to compromise the device locally or over the network.	9.8	More Details
CVE-2024-32353	TOTOLINK X5000R V9.1.0cu.2350_B20230313 was discovered to contain a command injection vulnerability via the 'port' parameter in the setSSServer function at /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2024-27939	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected systems allow the upload of arbitrary files of any unauthenticated user. An attacker could leverage this vulnerability and achieve arbitrary code execution with system privileges.	9.8	More Details
CVE-2024-34204	TOTOLINK outdoor CPE CP450 v4.1.0cu.747_B20191224 was discovered to contain a command injection vulnerability in the setUpgradeFW function via the FileName parameter.	9.8	More Details
CVE-2024-31473	There is a command injection vulnerability in the underlying deauthentication service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2024-30802	An issue in Vehicle Management System 7.31.0.3_20230412 allows an attacker to escalate privileges via the login.html component.	9.8	More Details
CVE-2022-32504	An issue was discovered on certain Nuki Home Solutions devices. The code used to parse the JSON objects received from the WebSocket service provided by the device leads to a stack buffer overflow. An attacker would be able to exploit this to gain arbitrary code execution on a KeyTurner device. This affects Nuki Smart Lock 3.0 before 3.3.5 and 2.0 before 2.12.4, as well as Nuki Bridge v1 before 1.22.0 and v2 before 2.13.2.	9.8	More Details
CVE-2024-25532	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the bt_id parameter at /include/get_dict.aspx.	9.8	More Details
CVE-2024-31961	A SQL injection vulnerability in unit.php in Sonic Shopfloor.guide before 3.1.3 allows remote attackers to execute arbitrary SQL commands via the level2 parameter.	9.8	More Details
CVE-2024-27280	A buffer-overread issue was discovered in StringIO 3.0.1, as distributed in Ruby 3.0.x through 3.0.6 and 3.1.x through 3.1.4. The ungetbyte and ungetc methods on a StringIO can read past the end of a string, and a subsequent call to StringIO.gets may return the memory value. 3.0.3 is the main fixed version; however, for Ruby 3.0 users, a fixed version is stringio 3.0.1.1, and for Ruby 3.1 users, a fixed version is stringio 3.0.1.2.	9.8	More Details
CVE-2024-28285	A Fault Injection vulnerability in the SymmetricDecrypt function in cryptopp/elgamal.h of Cryptopp Crypto++ 8.9, allows an attacker to co-reside in the same system with a victim process to disclose information and escalate privileges.	9.8	More Details
CVE-2024-29157	HDF5 through 1.14.3 contains a heap buffer overflow in H5HG_read, resulting in the corruption of the instruction pointer and causing denial of service or potential code execution.	9.8	More Details
CVE-2024-29159	HDF5 through 1.14.3 contains a buffer overflow in H5Z__filter_scaleoffset, resulting in the corruption of the instruction pointer and causing denial of service or potential code execution.	9.8	More Details
CVE-2024-25531	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the PageID parameter at /WebUtility/SearchCondiction.aspx.	9.8	More Details
CVE-2024-29164	HDF5 through 1.14.3 contains a stack buffer overflow in H5R__decode_heap, resulting in the corruption of the instruction pointer and causing denial of service or potential code execution.	9.8	More Details
CVE-2024-25530	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the PageID parameter at /WebUtility/get_find_condiction.aspx.	9.8	More Details
CVE-2024-25529	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the id parameter at /WorkFlow/wf_office_file_history_show.aspx.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34257	TOTOLINK EX1800T V9.1.0cu.2112_B20220316 has a vulnerability in the apcliEncrypType parameter that allows unauthorized execution of arbitrary commands, allowing an attacker to obtain device administrator privileges.	9.8	More Details
CVE-2024-32611	HDF5 Library through 1.14.3 may use an uninitialized value in H5A__attr_release_table in H5Aint.c.	9.8	More Details
CVE-2024-32113	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache OFBiz.This issue affects Apache OFBiz: before 18.12.13. Users are recommended to upgrade to version 18.12.13, which fixes the issue.	9.8	More Details
CVE-2024-32615	HDF5 Library through 1.14.3 contains a heap-based buffer overflow in H5Z__nbit_decompress_one_byte in H5Znbit.c, caused by the earlier use of an initialized pointer.	9.8	More Details
CVE-2024-25525	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the filename parameter at /WorkFlow/OfficeFileDownload.aspx.	9.8	More Details
CVE-2024-32621	HDF5 Library through 1.14.3 contains a heap-based buffer overflow in H5HG_read in H5HG.c (called from H5VL__native_blob_get in H5VLnative_blob.c), resulting in the corruption of the instruction pointer.	9.8	More Details
CVE-2024-25523	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the file_id parameter at /filemanage/file_memo.aspx.	9.8	More Details
CVE-2024-25520	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the id parameter at /SysManage/sys_blogtemplate_new.aspx.	9.8	More Details
CVE-2024-25519	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the idlist parameter at /WorkFlow/wf_work_print.aspx.	9.8	More Details
CVE-2024-32735	An issue regarding missing authentication for certain utilities exists in CyberPower PowerPanel Enterprise prior to v2.8.3. An unauthenticated remote attacker can access the PDNU REST APIs, which may result in compromise of the application.	9.8	More Details
CVE-2024-34716	PrestaShop is an open source e-commerce web application. A cross-site scripting (XSS) vulnerability that only affects PrestaShops with customer-thread feature flag enabled is present starting from PrestaShop 8.1.0 and prior to PrestaShop 8.1.6. When the customer thread feature flag is enabled through the front-office contact form, a hacker can upload a malicious file containing an XSS that will be executed when an admin opens the attached file in back office. The script injected can access the session and the security token, which allows it to perform any authenticated action in the scope of the administrator's right. This vulnerability is patched in 8.1.6. A workaround is to disable the customer-thread feature-flag.	9.6	More Details
CVE-2024-27107	Weak account password in GE HealthCare EchoPAC products	9.6	More Details
CVE-2024-33006	An unauthenticated attacker can upload a malicious file to the server which when accessed by a victim can allow an attacker to completely compromise system.	9.6	More Details
CVE-2024-30209	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected systems transmit client-side resources without proper cryptographic protection. This could allow an attacker to eavesdrop on and modify resources in transit. A successful exploit requires an attacker to be in the network path between the RTLS Locating Manager server and a client (MitM).	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34070	Froxlor is open source server administration software. Prior to 2.1.9, a Stored Blind Cross-Site Scripting (XSS) vulnerability was identified in the Failed Login Attempts Logging Feature of the Froxlor Application. An unauthenticated User can inject malicious scripts in the loginname parameter on the Login attempt, which will then be executed when viewed by the Administrator in the System Logs. By exploiting this vulnerability, the attacker can perform various malicious actions such as forcing the Administrator to execute actions without their knowledge or consent. For instance, the attacker can force the Administrator to add a new administrator controlled by the attacker, thereby giving the attacker full control over the application. This vulnerability is fixed in 2.1.9.	9.6	More Details
CVE-2024-34359	llama-cpp-python is the Python bindings for llama.cpp. `llama-cpp-python` depends on class `Llama` in `llama.py` to load `.gguf` llama.cpp or Latency Machine Learning Models. The `__init__` constructor built in the `Llama` takes several parameters to configure the loading and running of the model. Other than `NUMA, LoRa settings`, `loading tokenizers,` and `hardware settings`, `__init__` also loads the `chat template` from targeted `.gguf` 's Metadata and furtherly parses it to `llama_chat_format.Jinja2ChatFormatter.to_chat_handler()` to construct the `self.chat_handler` for this model. Nevertheless, `Jinja2ChatFormatter` parse the `chat template` within the Metadate with sandbox-less `jinja2.Environment`, which is furthermore rendered in `__call__` to construct the `prompt` of interaction. This allows `jinja2` Server Side Template Injection which leads to remote code execution by a carefully constructed payload.	9.6	More Details
CVE-2024-4671	Use after free in Visuals in Google Chrome prior to 124.0.6367.201 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2024-25518	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the template_id parameter at /WorkFlow/wf_get_fields_approve.aspx.	9.4	More Details
CVE-2024-25533	Error messages in RuvarOA v6.01 and v12.01 were discovered to leak the physical path of the website (/WorkFlow/OfficeFileUpdate.aspx). This vulnerability can allow attackers to write files to the server or execute arbitrary commands via crafted SQL statements.	9.4	More Details
CVE-2024-34226	SQL injection vulnerability in /php-sqlite-vms/?page=manage_visitor&id=1 in SourceCodester Visitor Management System 1.0 allow attackers to execute arbitrary SQL commands via the id parameters.	9.4	More Details
CVE-2024-25521	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the txt_keyword parameter at get_company.aspx.	9.4	More Details
CVE-2024-25522	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the office_missive_id parameter at /WorkFlow/wf_work_form_save.aspx.	9.4	More Details
CVE-2024-25524	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the sys_file_storage_id parameter at /WorkPlan/WorkPlanAttachDownLoad.aspx.	9.4	More Details
CVE-2024-22267	VMware Workstation and Fusion contain a use-after-free vulnerability in the vbluetooth device. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.	9.3	More Details
CVE-2024-32980	Spin is the developer tool for building and running serverless applications powered by WebAssembly. Prior to 2.4.3, some specifically configured Spin applications that use `self` requests without a specified URL authority can be induced to make requests to arbitrary hosts via the `Host` HTTP header. The following conditions need to be met for an application to be vulnerable: 1. The environment Spin is deployed in routes requests to the Spin runtime based on the request URL instead of the `Host` header, and leaves the `Host` header set to its original value; 2. The Spin application's component handling the incoming request is configured with an `allow_outbound_hosts` list containing `"self"`; and 3. In reaction to an incoming request, the component makes an outbound request whose URL doesn't include the hostname/port. Spin 2.4.3 has been released to fix this issue.	9.1	More Details
CVE-2024-32622	HDF5 Library through 1.14.3 contains a out-of-bounds read operation in H5FL_arr_malloc in H5FL.c (called from H5S_set_extent_simple in H5S.c).	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34340	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, Cacti calls `compat_password_hash` when users set their password. `compat_password_hash` use `password_hash` if there is it, else use `md5`. When verifying password, it calls `compat_password_verify`. In `compat_password_verify`, `password_verify` is called if there is it, else use `md5`. `password_verify` and `password_hash` are supported on PHP < 5.5.0, following PHP manual. The vulnerability is in `compat_password_verify`. Md5-hashed user input is compared with correct password in database by `$md5 == $hash`. It is a loose comparison, not `===`. It is a type juggling vulnerability. Version 1.2.27 contains a patch for the issue.	9.1	More Details
CVE-2024-34365	** UNSUPPORTED WHEN ASSIGNED ** Improper Input Validation vulnerability in Apache Karaf Cave.This issue affects all versions of Apache Karaf Cave. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an alternative or restrict access to the instance to trusted users.NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.1	More Details
CVE-2024-34416	Unrestricted Upload of File with Dangerous Type vulnerability in Pk Favicon Manager.This issue affects Pk Favicon Manager: from n/a through 2.1.	9.1	More Details
CVE-2024-34440	Unrestricted Upload of File with Dangerous Type vulnerability in Jordy Meow AI Engine: ChatGPT Chatbot.This issue affects AI Engine: ChatGPT Chatbot: from n/a through 2.2.63.	9.1	More Details
CVE-2024-34555	Unrestricted Upload of File with Dangerous Type vulnerability in URBAN BASE Z-Downloads.This issue affects Z-Downloads: from n/a through 1.11.3.	9.1	More Details
CVE-2024-2257	This vulnerability exists in Digisol Router (DG-GR1321: Hardware version 3.7L; Firmware version : v3.2.02) due to improper implementation of password policies. An attacker with physical access could exploit this by creating password that do not adhere to the defined security standards/policy on the vulnerable system. Successful exploitation of this vulnerability could allow the attacker to expose the router to potential security threats.	9.1	More Details
CVE-2024-35049	SurveyKing v1.3.1 was discovered to keep users' sessions active after logout. Related to an incomplete fix for CVE-2022-25590.	9.1	More Details
CVE-2024-3016	NEC Platforms DT900 and DT900S Series 5.0.0.0 – v5.3.4.4, v5.4.0.0 – v5.6.0.20 allows an attacker to access a non-documented the system settings to change settings via local network with unauthenticated user.	9.1	More Details
CVE-2024-33499	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). The affected application assigns incorrect permissions to a user management component. This could allow a privileged attacker to escalate their privileges from the Administrators group to the Systemadministrator group.	9.1	More Details
CVE-2024-26517	SQL Injection vulnerability in School Task Manager v.1.0 allows a remote attacker to obtain sensitive information via a crafted payload to the delete-task.php component.	9.1	More Details
CVE-2024-25641	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, an arbitrary file write vulnerability, exploitable through the "Package Import" feature, allows authenticated users having the "Import Templates" permission to execute arbitrary PHP code on the web server. The vulnerability is located within the `import_package()` function defined into the `/lib/import.php` script. The function blindly trusts the filename and file content provided within the XML data, and writes such files into the Cacti base path (or even outside, since path traversal sequences are not filtered). This can be exploited to write or overwrite arbitrary files on the web server, leading to execution of arbitrary PHP code or other security impacts. Version 1.2.27 contains a patch for this issue.	9.1	More Details
CVE-2023-47709	IBM Security Guardium 11.3, 11.4, 11.5, and 12.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 271524.	9.1	More Details
CVE-2024-32964	Lobe Chat is a chatbot framework that supports speech synthesis, multimodal, and extensible Function Call plugin system. Prior to 0.150.6, lobe-chat had an unauthorized Server-Side Request Forgery vulnerability in the /api/proxy endpoint. An attacker can construct malicious requests to cause Server-Side Request Forgery without logging in, attack intranet services, and leak sensitive information.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32002	Git is a revision control system. Prior to versions 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2, and 2.39.4, repositories with submodules can be crafted in a way that exploits a bug in Git whereby it can be fooled into writing files not into the submodule's worktree but into a `.git/` directory. This allows writing a hook that will be executed while the clone operation is still running, giving the user no opportunity to inspect the code that is being executed. The problem has been patched in versions 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2, and 2.39.4. If symbolic link support is disabled in Git (e.g. via `git config --global core.symlinks false`), the described attack won't work. As always, it is best to avoid cloning repositories from untrusted sources.	9.0	More Details
CVE-2024-28075	The SolarWinds Access Rights Manager was susceptible to Remote Code Execution Vulnerability. This vulnerability allows an authenticated user to abuse SolarWinds service resulting in remote code execution. We thank Trend Micro Zero Day Initiative (ZDI) for its ongoing partnership in coordinating with SolarWinds on responsible disclosure of this and other potential vulnerabilities.	9.0	More Details
CVE-2024-0087	NVIDIA Triton Inference Server for Linux contains a vulnerability where a user can set the logging location to an arbitrary file. If this file exists, logs are appended to the file. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-4129	Improper Authentication vulnerability in Snow Software AB Snow License Manager on Windows allows a networked attacker to perform an Authentication Bypass if Active Directory Authentication is enabled.This issue affects Snow License Manager: from 9.33.2 through 9.34.0.	8.8	More Details
CVE-2024-35010	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/banner_deal.php?mudi=del&dataType=&dataTypeCN=%E5%9B%BE%E7%89%87%E5%B9%BF%E5%91%8A&theme=cs&dataID=6.	8.8	More Details
CVE-2024-34921	TOTOLINK X5000R v9.1.0cu.2350_B20230313 was discovered to contain a command injection via the disconnectVPN function.	8.8	More Details
CVE-2024-34942	Tenda FH1206 V1.2.0.8(8155)_EN was discovered to contain a stack-based buffer overflow vulnerability via the funcpara1 parameter at ip/goform/exeCommand.	8.8	More Details
CVE-2024-34944	Tenda FH1206 V1.2.0.8(8155)_EN was discovered to contain a stack-based buffer overflow vulnerability via the list1 parameter at ip/goform/DhcpListClient.	8.8	More Details
CVE-2024-32605	HDF5 Library through 1.14.3 has a heap-based buffer over-read in H5VM_memcpyvv in H5VM.c (called from H5D__compact_readvv in H5Dcompact.c).	8.8	More Details
CVE-2024-30006	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-29161	HDF5 through 1.14.3 contains a heap buffer overflow in H5A__attr_release_table, resulting in the corruption of the instruction pointer and causing denial of service or potential code execution.	8.8	More Details
CVE-2024-3954	The Ditty plugin for WordPress is vulnerable to PHP Object Injection in all versions up to 3.1.38 via deserialization of untrusted input when adding a new ditty. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details
CVE-2024-35050	An issue in SurveyKing v1.3.1 allows attackers to escalate privileges via re-using the session ID of a user that was deleted by an Admin.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30007	Microsoft Brokering File System Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-31445	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, a SQL injection vulnerability in `automation_get_new_graphs_sql` function of `api_automation.php` allows authenticated users to exploit these SQL injection vulnerabilities to perform privilege escalation and remote code execution. In `api_automation.php` line 856, the `get_request_var('filter')` is being concatenated into the SQL statement without any sanitization. In `api_automation.php` line 717, The filter of `'filter'` is `FILTER_DEFAULT`, which means there is no filter for it. Version 1.2.27 contains a patch for the issue.	8.8	More Details
CVE-2023-33327	Improper Privilege Management vulnerability in Teplitsa of social technologies Leyka allows Privilege Escalation.This issue affects Leyka: from n/a through 3.30.2.	8.8	More Details
CVE-2024-32352	TOTOLINK X5000R V9.1.0cu.2350_B20230313 was discovered to contain an authenticated remote command execution (RCE) vulnerability via the "ipsecL2tpEnable" parameter in the "cstecgi.cgi" binary.	8.8	More Details
CVE-2024-27940	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected systems allow any authenticated user to send arbitrary SQL commands to the SQL server. An attacker could use this vulnerability to compromise the whole database.	8.8	More Details
CVE-2024-30206	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected SIMATIC RTLS Locating Manager Clients do not properly check the integrity of update files. This could allow an unauthenticated remote attacker to alter update files in transit and trick an authorized user into installing malicious code. A successful exploit requires the attacker to be able to modify the communication between server and client on the network.	8.8	More Details
CVE-2024-30009	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-35009	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/share_switch.php?mudi=switch&dataType=&fieldName=state&fieldName2=state&tabName=banner&dataID=6.	8.8	More Details
CVE-2024-34308	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a stack overflow via the password parameter in the function urldecode.	8.8	More Details
CVE-2022-32509	An issue was discovered on certain Nuki Home Solutions devices. Lack of certificate validation on HTTP communications allows attackers to intercept and tamper data. This affects Nuki Smart Lock 3.0 before 3.3.5, Nuki Bridge v1 before 1.22.0 and Nuki Bridge v2 before 2.13.2.	8.8	More Details
CVE-2024-3828	The Spectra Pro plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.1.5. This is due to the plugin allowing lower-privileged users to create registration forms and set the default role to administrator This makes it possible for authenticated attackers, with author-level access and above, to create administrator-level accounts.	8.8	More Details
CVE-2024-3809	The Porto Theme - Functionality plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.0.9 via the 'slideshow_type' post meta. This makes it possible for authenticated attackers, with contributor-level and above permissions, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where php file type can be uploaded and included.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3808	The Porto Theme - Functionality plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.1.0 via the 'porto_portfolios' shortcode 'portfolio_layout' attribute. This makes it possible for authenticated attackers, with contributor-level and above permissions, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where php file type can be uploaded and included.	8.8	More Details
CVE-2024-30010	Windows Hyper-V Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-31491	A client-side enforcement of server-side security in Fortinet FortiSandbox version 4.4.0 through 4.4.4 and 4.2.0 through 4.2.6 allows attacker to execute unauthorized code or commands via HTTP requests.	8.8	More Details
CVE-2024-3807	The Porto theme for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 7.1.0 via 'porto_page_header_shortcode_type', 'slideshow_type' and 'post_layout' post meta. This makes it possible for authenticated attackers, with contributor-level and above permissions, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where php file type can be uploaded and included. This was partially patched in version 7.1.0 and fully patched in version 7.1.1.	8.8	More Details
CVE-2024-30040	Windows MSHTML Platform Security Feature Bypass Vulnerability	8.8	More Details
CVE-2024-27941	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected client systems do not properly sanitize input data before sending it to the SQL server. An attacker could use this vulnerability to compromise the whole database.	8.8	More Details
CVE-2024-32614	HDF5 Library through 1.14.3 has a SEGV in H5VM_memcpyvv in H5VM.c.	8.8	More Details
CVE-2024-30017	Windows Hyper-V Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-34310	Jin Fang Times Content Management System v3.2.3 was discovered to contain a SQL injection vulnerability via the id parameter.	8.8	More Details
CVE-2024-2746	Incomplete fix for CVE-2024-1929 The problem with CVE-2024-1929 was that the dnf5 D-Bus daemon accepted arbitrary configuration parameters from unprivileged users, which allowed a local root exploit by tricking the daemon into loading a user controlled "plugin". All of this happened before Polkit authentication was even started. The dnf5 library code does not check whether non-root users control the directory in question. On one hand, this poses a Denial-of-Service attack vector by making the daemonoperate on a blocking file (e.g. named FIFO special file) or a very large file that causes an out-of-memory situation (e.g. /dev/zero). On the other hand, this can be used to let the daemon process privileged files like /etc/shadow. The file in question is parsed as an INI file. Error diagnostics resulting from parsing privileged files could cause information leaks, if these diagnostics are accessible to unprivileged users. In the case of libdnf5, no such user accessible diagnostics should exist, though. Also, a local attacker can place a valid repository configuration file in this directory. This configuration file allows to specify a plethora of additional configuration options. This makes various additional code paths in libdnf5 accessible to the attacker.	8.8	More Details
CVE-2024-34221	Sourcecodester Human Resource Management System 1.0 is vulnerable to Insecure Permissions resulting in privilege escalation.	8.8	More Details
CVE-2024-34211	TOTOLINK CP450 v4.1.0cu.747_B20191224 was discovered to contain a hardcoded password vulnerability in /etc/shadow.sample, which allows attackers to log in as root.	8.8	More Details
CVE-2024-34207	TOTOLINK CP450 v4.1.0cu.747_B20191224 was discovered to contain a stack buffer overflow vulnerability in the setStaticDhcpConfig function.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34200	TOTOLINK CPE CP450 v4.1.0cu.747_B20191224 was discovered to contain a stack buffer overflow vulnerability in the setIpQosRules function.	8.8	More Details
CVE-2024-32351	TOTOLINK X5000R V9.1.0cu.2350_B20230313 was discovered to contain an authenticated remote command execution (RCE) vulnerability via the "mru" parameter in the "cstecgi.cgi" binary.	8.8	More Details
CVE-2024-34196	Totolink AC1200 Wireless Dual Band Gigabit Router A3002RU_V3 Firmware V3.0.0-B20230809.1615 is vulnerable to Buffer Overflow. The "boa" program allows attackers to modify the value of the "vwlan_idx" field via "formMultiAP". This can lead to a stack overflow through the "formWlEncrypt" CGI function by constructing malicious HTTP requests and passing a WLAN SSID value exceeding the expected length, potentially resulting in command execution or denial of service attacks.	8.8	More Details
CVE-2024-32617	HDF5 Library through 1.14.3 contains a heap-based buffer over-read caused by the unsafe use of strdup in H5MM_xstrdup in H5MM.c (called from H5G__ent_to_link in H5Glink.c).	8.8	More Details
CVE-2024-4397	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'save_post_materials' function in versions up to, and including, 4.2.6.5. This makes it possible for authenticated attackers, with Instructor-level permissions and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2024-3055	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to time-based SQL Injection via the ‘id’ parameter in all versions up to, and including, 1.5.102 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 access or higher, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2022-32507	An issue was discovered on certain Nuki Home Solutions devices. Some BLE commands, which should have been designed to be only called from privileged accounts, could also be called from unprivileged accounts. This demonstrates that no access controls were implemented for the different BLE commands across the different accounts. This affects Nuki Smart Lock 3.0 before 3.3.5 and Nuki Smart Lock 2.0 before 2.12.4.	8.8	More Details
CVE-2024-33877	HDF5 Library through 1.14.3 has a heap-based buffer overflow in H5T__conv_struct_opt in H5Tconv.c.	8.8	More Details
CVE-2024-33873	HDF5 Library through 1.14.3 has a heap-based buffer overflow in H5D__scatter_mem in H5Dscatgath.c.	8.8	More Details
CVE-2024-32350	TOTOLINK X5000R V9.1.0cu.2350_B20230313 was discovered to contain an authenticated remote command execution (RCE) vulnerability via the "ipsecPsk" parameter in the "cstecgi.cgi" binary.	8.8	More Details
CVE-2024-4770	When saving a page to PDF, certain font styles could have led to a potential use-after-free crash. This vulnerability affects Firefox < 126, Firefox ESR < 115.11, and Thunderbird < 115.11.	8.8	More Details
CVE-2024-4761	Out of bounds write in V8 in Google Chrome prior to 124.0.6367.207 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-4605	The Breakdance plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.7.1 via post meta data. This is due to the plugin storing custom data in metadata without an underscore prefix. This makes it possible for lower privileged users, such as contributors, to edit this data via UI. As a result they can escalate their privileges or execute arbitrary code.	8.8	More Details
CVE-2024-32623	HDF5 Library through 1.14.3 contains a heap-based buffer overflow in H5VM_array_fill in H5VM.c (called from H5S_select_elements in H5Spoint.c).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27813	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.5. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges.	8.6	More Details
CVE-2024-34199	TinyWeb 1.94 and below allows unauthenticated remote attackers to cause a denial of service (Buffer Overflow) when sending excessively large elements in the request line.	8.6	More Details
CVE-2024-4771	A memory allocation check was missing which would lead to a use-after-free if the allocation failed. This could have triggered a crash or potentially be leveraged to achieve code execution. This vulnerability affects Firefox < 126.	8.6	More Details
CVE-2024-34219	TOTOLINK CP450 V4.1.0cu.747_B20191224 was discovered to contain a vulnerability in the SetTelnetCfg function, which allows attackers to log in through telnet.	8.6	More Details
CVE-2024-23473	The SolarWinds Access Rights Manager was found to contain a hard-coded credential authentication bypass vulnerability. If exploited, this vulnerability allows access to the RabbitMQ management console. We thank Trend Micro Zero Day Initiative (ZDI) for its ongoing partnership in coordinating with SolarWinds on responsible disclosure of this and other potential vulnerabilities.	8.6	More Details
CVE-2023-26566	Sangoma FreePBX 1805 through 2203 on Linux contains hardcoded credentials for the Asterisk REST Interface (ARI), which allows remote attackers to reconfigure Asterisk and make external and internal calls via HTTP and WebSocket requests sent to the API.	8.6	More Details
CVE-2024-3459	KioWare for Windows (versions all through 8.34) allows to escape the environment by downloading PDF files, which then by default are opened in an external PDF viewer. By using built-in functions of that viewer it is possible to launch a web browser, search through local files and, subsequently, launch any program with user privileges.	8.4	More Details
CVE-2024-27110	Elevation of privilege vulnerability in GE HealthCare EchoPAC products	8.4	More Details
CVE-2024-35204	Veritas System Recovery before 23.3_Hotfix has incorrect permissions for the Veritas System Recovery folder, and thus low-privileged users can conduct attacks.	8.4	More Details
CVE-2024-32997	Race condition vulnerability in the binder driver module Impact: Successful exploitation of this vulnerability will affect availability.	8.4	More Details
CVE-2024-1628	OS command injection vulnerabilities in GE HealthCare ultrasound devices	8.4	More Details
CVE-2024-22064	ZTE ZXUN-ePDG product, which serves as the network node of the VoWifi system, under by default configuration, uses a set of non-unique cryptographic keys during establishing a secure connection(IKE) with the mobile devices connecting over the internet . If the set of keys are leaked or cracked, the user session informations using the keys may be leaked.	8.3	More Details
CVE-2024-34347	@hoppscotch/cli is a CLI to run Hoppscotch Test Scripts in CI environments. Prior to 0.8.0, the @hoppscotch/js-sandbox package provides a Javascript sandbox that uses the Node.js vm module. However, the vm module is not safe for sandboxing untrusted Javascript code. This is because code inside the vm context can break out if it can get a hold of any reference to an object created outside of the vm. In the case of @hoppscotch/js-sandbox, multiple references to external objects are passed into the vm context to allow pre-request scripts interactions with environment variables and more. But this also allows the pre-request script to escape the sandbox. This vulnerability is fixed in 0.8.0.	8.3	More Details
CVE-2024-3727	A flaw was found in the github.com/containers/image library. This flaw allows attackers to trigger unexpected authenticated registry accesses on behalf of a victim user, causing resource exhaustion, local path traversal, and other attacks.	8.3	More Details
CVE-2024-4776	A file dialog shown while in full-screen mode could have resulted in the window remaining disabled. This vulnerability affects Firefox < 126.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30258	FastDDS is a C++ implementation of the DDS (Data Distribution Service) standard of the OMG (Object Management Group). Prior to versions 2.14.1, 2.13.5, 2.10.4, and 2.6.8, when a publisher serves a malformed `RTPS` packet, the subscriber crashes when creating `pthread`. This can remotely crash any Fast-DDS process, potentially leading to a DOS attack. Versions 2.14.1, 2.13.5, 2.10.4, and 2.6.8 contain a patch for the issue.	8.2	More Details
CVE-2024-30259	FastDDS is a C++ implementation of the DDS (Data Distribution Service) standard of the OMG (Object Management Group). Prior to versions 2.14.1, 2.13.5, 2.10.4, and 2.6.8, when a publisher serves malformed `RTPS` packet, heap buffer overflow occurs on the subscriber. This can remotely crash any Fast-DDS process, potentially leading to a DOS attack. Versions 2.14.1, 2.13.5, 2.10.4, and 2.6.8 contain a patch for the issue.	8.2	More Details
CVE-2024-34974	Tenda AC18 v15.03.05.19 is vulnerable to Buffer Overflow in the formSetPPTPServer function via the endIp parameter.	8.2	More Details
CVE-2024-31474	There is an arbitrary file deletion vulnerability in the CLI service accessed by PAPI (Aruba's Access Point management protocol). Successful exploitation of this vulnerability results in the ability to delete arbitrary files on the underlying operating system, which could lead to the ability to interrupt normal operation and impact the integrity of the affected Access Point	8.2	More Details
CVE-2024-34360	go-spacemesh is a Go implementation of the Spacemesh protocol full node. Nodes can publish activations transactions (ATXs) which reference the incorrect previous ATX of the Smesher that created the ATX. ATXs are expected to form a single chain from the newest to the first ATX ever published by an identity. Allowing Smeshers to reference an earlier (but not the latest) ATX as previous breaks this protocol rule and can serve as an attack vector where Nodes are rewarded for holding their PoST data for less than one epoch but still being eligible for rewards. This vulnerability is fixed in go-spacemesh 1.5.2-hotfix1 and Spacemesh API 1.37.1.	8.2	More Details
CVE-2024-31475	There is an arbitrary file deletion vulnerability in the Central Communications service accessed by PAPI (Aruba's access point management protocol). Successful exploitation of this vulnerability results in the ability to delete arbitrary files on the underlying operating system, which could lead to the ability to interrupt normal operation and impact the integrity of the affected Access Point.	8.2	More Details
CVE-2024-4765	Web application manifests were stored by using an insecure MD5 hash which allowed for a hash collision to overwrite another application's manifest. This could have been exploited to run arbitrary code in another application's context. *This issue only affects Firefox for Android. Other versions of Firefox are unaffected.* This vulnerability affects Firefox < 126.	8.1	More Details
CVE-2020-26312	Dotmesh is a git-like command-line interface for capturing, organizing and sharing application states. In versions 0.8.1 and prior, the unsafe handling of symbolic links in an unpacking routine may enable attackers to read and/or write to arbitrary locations outside the designated target folder. The routine `untarFile` attempts to guard against creating symbolic links that point outside the directory a tar archive is extracted to. However, a malicious tarball first linking `subdir/parent` to `..` (allowed, because `subdir/..` falls within the archive root) and then linking `subdir/parent/escapes` to `..` results in a symbolic link pointing to the tarball’s parent directory, contrary to the routine’s goals. This issue may lead to arbitrary file write (with same permissions as the program running the unpack operation) if the attacker can control the archive file. Additionally, if the attacker has read access to the unpacked files, they may be able to read arbitrary system files the parent process has permissions to read. As of time of publication, no patch for this issue is available.	8.1	More Details
CVE-2024-30020	Windows Cryptographic Services Remote Code Execution Vulnerability	8.1	More Details
CVE-2024-4441	The XML Sitemap & Google News plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 5.4.8 via the 'feed' parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	8.1	More Details
CVE-2024-25526	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the project_id parameter at /ProjectManage/pm_gatt_inc.aspx.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32004	Git is a revision control system. Prior to versions 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2, and 2.39.4, an attacker can prepare a local repository in such a way that, when cloned, will execute arbitrary code during the operation. The problem has been patched in versions 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2, and 2.39.4. As a workaround, avoid cloning repositories from untrusted sources.	8.1	More Details
CVE-2024-32655	Npgsql is the .NET data provider for PostgreSQL. The `WriteBind()` method in `src/Npgsql/Internal/NpgsqlConnector.FrontendMessages.cs` uses `int` variables to store the message length and the sum of parameter lengths. Both variables overflow when the sum of parameter lengths becomes too large. This causes Npgsql to write a message size that is too small when constructing a Postgres protocol message to send it over the network to the database. When parsing the message, the database will only read a small number of bytes and treat any following bytes as new messages while they belong to the old message. Attackers can abuse this to inject arbitrary Postgres protocol messages into the connection, leading to the execution of arbitrary SQL statements on the application's behalf. This vulnerability is fixed in 4.0.14, 4.1.13, 5.0.18, 6.0.11, 7.0.7, and 8.0.3.	8.1	More Details
CVE-2024-34345	The CycloneDX JavaScript library contains the core functionality of OWASP CycloneDX for JavaScript. In 6.7.0, XML External entity injections were possible, when running the provided XML Validator on arbitrary input. This issue was fixed in version 6.7.1.	8.1	More Details
CVE-2024-28165	SAP Business Objects Business Intelligence Platform is vulnerable to stored XSS allowing an attacker to manipulate a parameter in the Opendocument URL which could lead to high impact on Confidentiality and Integrity of the application	8.1	More Details
CVE-2020-18305	Extreme Networks EXOS before v.22.7 and before v.30.2 was discovered to contain an issue in its Web GUI which fails to restrict URL access, allowing attackers to access sensitive information or escalate privileges.	8.0	More Details
CVE-2024-31156	A stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.0	More Details
CVE-2024-29800	Deserialization of Untrusted Data vulnerability in Timber Team & Contributors Timber.This issue affects Timber: from n/a through 1.23.0.	8.0	More Details
CVE-2024-32355	TOTOLINK X5000R V9.1.0cu.2350_B20230313 was discovered to contain a command injection vulnerability via the 'password' parameter in the setSSServer function.	8.0	More Details
CVE-2024-31459	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, there is a file inclusion issue in the `lib/plugin.php` file. Combined with SQL injection vulnerabilities, remote code execution can be implemented. There is a file inclusion issue with the `api_plugin_hook()` function in the `lib/plugin.php` file, which reads the plugin_hooks and plugin_config tables in database. The read data is directly used to concatenate the file path which is used for file inclusion. Version 1.2.27 contains a patch for the issue.	8.0	More Details
CVE-2024-29994	Microsoft Windows SCSI Class System File Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-30035	Windows DWM Core Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-34085	A vulnerability has been identified in JT2Go (All versions < V2312.0001), Teamcenter Visualization V14.1 (All versions < V14.1.0.13), Teamcenter Visualization V14.2 (All versions < V14.2.0.10), Teamcenter Visualization V14.3 (All versions < V14.3.0.7), Teamcenter Visualization V2312 (All versions < V2312.0001). The affected applications contain a stack overflow vulnerability while parsing specially crafted XML files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-30038	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-22774	An issue in Panoramic Corporation Digital Imaging Software v.9.1.2.7600 allows a local attacker to escalate privileges via the ccsservice.exe component.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4044	A deserialization of untrusted data vulnerability exists in common code used by FlexLogger and InstrumentStudio that may result in remote code execution. Successful exploitation requires an attacker to get a user to open a specially crafted project file. This vulnerability affects NI FlexLogger 2024 Q1 and prior versions as well as NI InstrumentStudio 2024 Q1 and prior versions.	7.8	More Details
CVE-2024-33577	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain a stack overflow vulnerability while parsing specially strings as argument for one of the application binaries. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-30042	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-33493	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 5). 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-2024-33492	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 5). 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-2024-30032	Windows DWM Core Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-34772	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 4). 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-2024-30031	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-30030	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-26238	Microsoft PLUGScheduler Scheduled Task Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-35841	Exposed IOCTL with Insufficient Access Control in Phoenix WinFlash Driver on Windows allows Privilege Escalation which allows for modification of system firmware.This issue affects WinFlash Driver: before 4.5.0.0.	7.8	More Details
CVE-2024-29996	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-31771	Insecure Permission vulnerability in TotalAV v.6.0.740 allows a local attacker to escalate privileges via a crafted file	7.8	More Details
CVE-2024-35205	The WPS Office (aka cn.wps.moffice_eng) application before 17.0.0 for Android fails to properly sanitize file names before processing them through external application interactions, leading to a form of path traversal. This potentially enables any application to dispatch a crafted library file, aiming to overwrite an existing native library utilized by WPS Office. Successful exploitation could result in the execution of arbitrary commands under the guise of WPS Office's application ID.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3037	An arbitrary file deletion vulnerability exists in PaperCut NG/MF, specifically affecting Windows servers with Web Print enabled. To exploit this vulnerability, an attacker must first obtain local login access to the Windows Server hosting PaperCut NG/MF and be capable of executing low-privilege code directly on the server. Important: In most installations, this risk is mitigated by the default Windows Server configuration, which typically restricts local login access to Administrators only. However, this vulnerability could pose a risk to customers who allow non-administrative users to log in to the local console of the Windows environment hosting the PaperCut NG/MF application server. Note: This CVE has been split into two separate CVEs (CVE-2024-3037 and CVE-2024-8404) and it's been rescored with a "Privileges Required (PR)" rating of low, and "Attack Complexity (AC)" rating of low, reflecting the worst-case scenario where an Administrator has granted local login access to standard users on the host server.	7.8	More Details
CVE-2024-34773	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 2). 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-2024-29513	An issue in briscKernelDriver.sys in BlueRiSC WindowsSCOPE Cyber Forensics before 3.3 allows a local attacker to execute arbitrary code within the driver and create a local denial-of-service condition due to an improper DACL being applied to the device the driver creates.	7.8	More Details
CVE-2024-33490	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 5). 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-2024-30018	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-34771	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 2). 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-2024-27843	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.5. An app may be able to elevate privileges.	7.8	More Details
CVE-2024-27842	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2024-30025	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-27829	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.5. Processing a file may lead to unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2024-27824	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.5. An app may be able to elevate privileges.	7.8	More Details
CVE-2024-27822	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sonoma 14.5. An app may be able to gain root privileges.	7.8	More Details
CVE-2024-30027	NTFS Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-27818	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.5 and iPadOS 17.5, macOS Sonoma 14.5. An attacker may be able to cause unexpected app termination or arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34086	A vulnerability has been identified in JT2Go (All versions < V2312.0001), Teamcenter Visualization V14.1 (All versions < V14.1.0.13), Teamcenter Visualization V14.2 (All versions < V14.2.0.10), Teamcenter Visualization V14.3 (All versions < V14.3.0.7), Teamcenter Visualization V2312 (All versions < V2312.0001). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted CGM file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-30028	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-27796	The issue was addressed with improved checks. This issue is fixed in iOS 17.5 and iPadOS 17.5, macOS Sonoma 14.5. An attacker may be able to elevate privileges.	7.8	More Details
CVE-2024-27793	The issue was addressed with improved checks. This issue is fixed in iTunes 12.13.2 for Windows. Parsing a file may lead to an unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2024-33491	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 5). 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-2024-27798	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.5. An attacker may be able to elevate privileges.	7.8	More Details
CVE-2024-32063	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected application contains a type confusion vulnerability while parsing IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21573)	7.8	More Details
CVE-2024-32066	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21578)	7.8	More Details
CVE-2024-32636	A vulnerability has been identified in JT2Go (All versions < V2312.0005), Teamcenter Visualization V14.2 (All versions < V14.2.0.12), Teamcenter Visualization V14.3 (All versions < V14.3.0.10), Teamcenter Visualization V2312 (All versions < V2312.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-33489	A vulnerability has been identified in Solid Edge (All versions < V224.0 Update 5). 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-2024-28136	A local attacker with low privileges can use a command injection vulnerability to gain root privileges due to improper input validation using the OCPP Remote service.	7.8	More Details
CVE-2024-32635	A vulnerability has been identified in JT2Go (All versions < V2312.0005), Teamcenter Visualization V14.2 (All versions < V14.2.0.12), Teamcenter Visualization V14.3 (All versions < V14.3.0.10), Teamcenter Visualization V2312 (All versions < V2312.0005). The affected applications contain an out of bounds read past the unmapped memory region while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-28133	A local low privileged attacker can use an untrusted search path in a CHARX system utility to gain root privileges.	7.8	More Details
CVE-2024-31980	A vulnerability has been identified in Parasolid V35.1 (All versions < V35.1.256), Parasolid V36.0 (All versions < V36.0.210), Parasolid V36.1 (All versions < V36.1.185). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted X_T part file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-23468)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32055	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-32065	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21577)	7.8	More Details
CVE-2024-32639	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0011). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted MODEL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-22974)	7.8	More Details
CVE-2024-32064	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21575)	7.8	More Details
CVE-2024-32057	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected application contains a type confusion vulnerability while parsing IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21562)	7.8	More Details
CVE-2024-32062	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected application contains a type confusion vulnerability while parsing IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21568)	7.8	More Details
CVE-2024-32061	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21566)	7.8	More Details
CVE-2024-32060	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21565)	7.8	More Details
CVE-2024-32059	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21564)	7.8	More Details
CVE-2024-32058	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected application is vulnerable to memory corruption while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21563)	7.8	More Details
CVE-2023-47712	IBM Security Guardium 11.3, 11.4, 11.5, and 12.0 could allow a local user to gain elevated privileges on the system due to improper permissions control. IBM X-Force ID: 271527.	7.8	More Details
CVE-2024-28137	A local attacker with low privileges can perform a privilege escalation with an init script due to a TOCTOU vulnerability.	7.8	More Details
CVE-2024-30051	Windows DWM Core Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-30049	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-4712	An arbitrary file creation vulnerability exists in PaperCut NG/MF that only affects Windows servers with Web Print enabled. This specific flaw exists within the image-handler process, which can incorrectly create files that don’t exist when a maliciously formed payload is provided. This can lead to local privilege escalation. Note: This CVE has been split into two (CVE-2024-4712 and CVE-2024-8405) and it’s been rescored with a "Privileges Required (PR)" rating of low, and “Attack Complexity (AC)” rating of low, reflecting the worst-case scenario where an Administrator has granted local login access to standard network users on the host server.	7.8	More Details
CVE-2024-2860	The PostgreSQL implementation in Brocade SANnav versions before 2.3.0a is vulnerable to an incorrect local authentication flaw. An attacker accessing the VM where the Brocade SANnav is installed can gain access to sensitive data inside the PostgreSQL database.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31556	An issue in Reportico Web before v.8.1.0 allows a local attacker to execute arbitrary code and obtain sensitive information via the sessionid function.	7.8	More Details
CVE-2024-31484	A vulnerability has been identified in CPC80 Central Processing/Communication (All versions < V16.41), CPCI85 Central Processing/Communication (All versions < V5.30), CPCX26 Central Processing/Communication (All versions < V06.02), ETA4 Ethernet Interface IEC60870-5-104 (All versions < V10.46), ETA5 Ethernet Int. 1x100TX IEC61850 Ed.2 (All versions < V03.27), PCCX26 Ax 1703 PE, Contr, Communication Element (All versions < V06.05). The affected devices contain an improper null termination vulnerability while parsing a specific HTTP header. This could allow an attacker to execute code in the context of the current process or lead to denial of service condition.	7.8	More Details
CVE-2024-34217	TOTOLINK CP450 v4.1.0cu.747_B20191224 was discovered to contain a stack buffer overflow vulnerability in the addWlProfileClientMode function.	7.7	More Details
CVE-2024-1630	Path traversal vulnerability in “getAllFolderContents” function of Common Service Desktop, a GE HealthCare ultrasound device component	7.7	More Details
CVE-2024-1438	Missing Authorization vulnerability in PressFore Rolo Slider.This issue affects Rolo Slider: from n/a through 1.0.9.	7.7	More Details
CVE-2024-3507	Improper privilege management vulnerability in Lunar software that affects versions 6.0.2 through 6.6.0. This vulnerability allows an attacker to perform a secondary process injection into the Lunar application and abuse those rights to access sensitive user information.	7.7	More Details
CVE-2024-4545	All versions of EnterpriseDB Postgres Advanced Server (EPAS) from 15.0 prior to 15.7.0 and from 16.0 prior to 16.3.0 may allow users using edbldr to bypass role permissions from pg_read_server_files. This could allow low privilege users to read files to which they would not otherwise have access.	7.7	More Details
CVE-2022-4967	strongSwan versions 5.9.2 through 5.9.5 are affected by authorization bypass through improper validation of certificate with host mismatch (CWE-297). When certificates are used to authenticate clients in TLS-based EAP methods, the IKE or EAP identity supplied by a client is not enforced to be contained in the client's certificate. So clients can authenticate with any trusted certificate and claim an arbitrary IKE/EAP identity as their own. This is problematic if the identity is used to make policy decisions. A fix was released in strongSwan version 5.9.6 in August 2022 (e4b4aabc4996fc61c37deab7858d07bc4d220136).	7.7	More Details
CVE-2024-30047	Dynamics 365 Customer Insights Spoofing Vulnerability	7.6	More Details
CVE-2022-32503	An issue was discovered on certain Nuki Home Solutions devices. An attacker with physical access to this JTAG port may be able to connect to the device and bypass both hardware and software security protections. This affects Nuki Keypad before 1.9.2 and Nuki Fob before 1.8.1.	7.6	More Details
CVE-2024-30048	Dynamics 365 Customer Insights Spoofing Vulnerability	7.6	More Details
CVE-2024-34697	FreeScout is a free, self-hosted help desk and shared mailbox. A stored HTML Injection vulnerability has been identified in the Email Receival Module of the Freescout Application. The vulnerability allows attackers to inject malicious HTML content into emails sent to the application's mailbox. This vulnerability arises from improper handling of HTML content within incoming emails, allowing attackers to embed malicious HTML code in the context of the application's domain. Unauthenticated attackers can exploit this vulnerability to inject malicious HTML content into emails. This could lead to various attacks such as form hijacking, application defacement, or data exfiltration via CSS injection. Although unauthenticated attackers are limited to HTML injection, the consequences can still be severe. Version 1.8.139 implements strict input validation and sanitization mechanisms to ensure that any HTML content received via emails is properly sanitized to prevent malicious HTML injections.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1913	An attacker who successfully exploited these vulnerabilities could cause the robot to stop, make the robot controller inaccessible, or execute arbitrary code. The vulnerability could potentially be exploited to perform unauthorized actions by an attacker. This vulnerability arises under specific condition when specially crafted message is processed by the system. Below are reported vulnerabilities in the Robot Ware versions. * IRC5- RobotWare 6 < 6.15.06 except 6.10.10, and 6.13.07 * OmniCore- RobotWare 7 < 7.14	7.6	More Details
CVE-2024-32742	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V3.0). The affected device contains an unrestricted USB port. An attacker with local access to the device could potentially misuse the port for booting another operating system and gain complete read/write access to the filesystem.	7.6	More Details
CVE-2024-27109	Insufficiently protected credentials in GE HealthCare EchoPAC products	7.6	More Details
CVE-2024-31270	Missing Authorization vulnerability in Repute InfoSystems ARForms Form Builder.This issue affects ARForms Form Builder: from n/a through 1.6.1.	7.6	More Details
CVE-2024-27082	Cacti provides an operational monitoring and fault management framework. Versions of Cacti prior to 1.2.27 are vulnerable to stored cross-site scripting, a type of cross-site scripting where malicious scripts are permanently stored on a target server and served to users who access a particular page. Version 1.2.27 contains a patch for the issue.	7.6	More Details
CVE-2024-34714	The Hoppscotch Browser Extension is a browser extension for Hoppscotch, a community-driven end-to-end open-source API development ecosystem. Due to an oversight during a change made to the extension in the commit d4e8e4830326f46ba17acd1307977ecd32a85b58, a critical check for the origin list was missed and allowed for messages to be sent to the extension which the extension gladly processed and responded back with the results of, while this wasn't supposed to happen and be blocked by the origin not being present in the origin list. This vulnerability exposes Hoppscotch Extension users to sites which call into Hoppscotch Extension APIs internally. This fundamentally allows any site running on the browser with the extension installed to bypass CORS restrictions if the user is running extensions with the given version. This security hole was patched in the commit 7e364b928ab722dc682d0fcad713a96cc38477d6 which was released along with the extension version `0.35`. As a workaround, Chrome users can use the Extensions Settings to disable the extension access to only the origins that you want. Firefox doesn't have an alternative to upgrading to a fixed version.	7.6	More Details
CVE-2024-34950	D-Link DIR-822+ v1.0.5 was discovered to contain a stack-based buffer overflow vulnerability in the SetNetworkTomographySettings module.	7.5	More Details
CVE-2024-4773	When a network error occurred during page load, the prior content could have remained in view with a blank URL bar. This could have been used to obfuscate a spoofed web site. This vulnerability affects Firefox < 126.	7.5	More Details
CVE-2024-33608	When IPsec is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2024-30022	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	7.5	More Details
CVE-2024-30015	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	7.5	More Details
CVE-2024-34559	Insertion of Sensitive Information into Log File vulnerability in Ghost Foundation Ghost.This issue affects Ghost: from n/a through 1.4.0.	7.5	More Details
CVE-2024-31441	DataEase is an open source data visualization analysis tool. Due to the lack of restrictions on the connection parameters for the ClickHouse data source, it is possible to exploit certain malicious parameters to achieve arbitrary file reading. The vulnerability has been fixed in v1.18.19.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4437	The etcd package distributed with the Red Hat OpenStack platform has an incomplete fix for CVE-2021-44716. This issue occurs because the etcd package in the Red Hat OpenStack platform is using http://golang.org/x/net/http2 instead of the one provided by Red Hat Enterprise Linux versions, meaning it should be updated at compile time instead.	7.5	More Details
CVE-2024-32736	A sql injection vulnerability exists in CyberPower PowerPanel Enterprise prior to v2.8.3. An unauthenticated remote attacker can leak sensitive information via the "query_utask_verbose" function within MCUDBHelper.	7.5	More Details
CVE-2024-29857	An issue was discovered in ECCurve.java and ECCurve.cs in Bouncy Castle Java (BC Java) before 1.78, BC Java LTS before 2.73.6, BC-FJA before 1.0.2.5, and BC C# .Net before 2.3.1. Importing an EC certificate with crafted F2m parameters can lead to excessive CPU consumption during the evaluation of the curve parameters.	7.5	More Details
CVE-2024-34459	An issue was discovered in xmllint (from libxml2) before 2.11.8 and 2.12.x before 2.12.7. Formatting error messages with xmllint --htmlout can result in a buffer over-read in xmlHTMLPrintFileContext in xmllint.c.	7.5	More Details
CVE-2024-26026	An SQL injection vulnerability exists in the BIG-IP Next Central Manager API (URI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.5	More Details
CVE-2024-4438	The etcd package distributed with the Red Hat OpenStack platform has an incomplete fix for CVE-2023-39325/CVE-2023-44487, known as Rapid Reset. This issue occurs because the etcd package in the Red Hat OpenStack platform is using http://golang.org/x/net/http2 instead of the one provided by Red Hat Enterprise Linux versions, meaning it should be updated at compile time instead.	7.5	More Details
CVE-2024-30023	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	7.5	More Details
CVE-2024-25560	When BIG-IP AFM is licensed and provisioned, undisclosed DNS traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2024-1929	Local Root Exploit via Configuration Dictionary in dnf5daemon-server before 5.1.17 allows a malicious user to impact Confidentiality and Integrity via Configuration Dictionary. There are issues with the D-Bus interface long before Polkit is invoked. The `org.rpm.dnf.v0.SessionManager.open_session` method takes a key/value map of configuration entries. A sub-entry in this map, placed under the "config" key, is another key/value map. The configuration values found in it will be forwarded as configuration overrides to the `libdnf5::Base` configuration. Practically all libdnf5 configuration aspects can be influenced here. Already when opening the session via D-Bus, the libdnf5 will be initialized using these override configuration values. There is no sanity checking of the content of this "config" map, which is untrusted data. It is possible to make the library loading a plug-in shared library under control of an unprivileged user, hence achieving root access.	7.5	More Details
CVE-2024-30014	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	7.5	More Details
CVE-2024-21793	An OData injection vulnerability exists in the BIG-IP Next Central Manager API (URI). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2024-32609	HDF5 Library through 1.14.3 allows stack consumption in the function H5E_printf_stack in H5Eint.c.	7.5	More Details
CVE-2024-32737	A sql injection vulnerability exists in CyberPower PowerPanel Enterprise prior to v2.8.3. An unauthenticated remote attacker can leak sensitive information via the "query_contract_result" function within MCUDBHelper.	7.5	More Details
CVE-2024-30024	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4436	The etcd package distributed with the Red Hat OpenStack platform has an incomplete fix for CVE-2022-41723. This issue occurs because the etcd package in the Red Hat OpenStack platform is using http://golang.org/x/net/http2 instead of the one provided by Red Hat Enterprise Linux versions, meaning it should be updated at compile time instead.	7.5	More Details
CVE-2024-32724	Missing Authorization vulnerability in Woo product importer Sharkdropship dropshipping for Aliexpress, eBay, Amazon, etsy.This issue affects Sharkdropship dropshipping for Aliexpress, eBay, Amazon, etsy: from n/a through 2.1.1.	7.5	More Details
CVE-2024-0096	NVIDIA ChatRTX for Windows contains a vulnerability in Chat RTX UI, where a user can cause an improper privilege management issue by sending user inputs to change execution flow. A successful exploit of this vulnerability might lead to information disclosure, escalation of privileges, and data tampering.	7.5	More Details
CVE-2024-0097	NVIDIA ChatRTX for Windows contains a vulnerability in ChatRTX UI, where a user can cause an improper privilege management issue by exploiting interprocess communication between different processes. A successful exploit of this vulnerability might lead to information disclosure, escalation of privileges, and data tampering.	7.5	More Details
CVE-2024-0762	Potential buffer overflow in unsafe UEFI variable handling in Phoenix SecureCore™ for select Intel platforms This issue affects: Phoenix SecureCore™ for Intel Kaby Lake: from 4.0.1.1 before 4.0.1.998; Phoenix SecureCore™ for Intel Coffee Lake: from 4.1.0.1 before 4.1.0.562; Phoenix SecureCore™ for Intel Ice Lake: from 4.2.0.1 before 4.2.0.323; Phoenix SecureCore™ for Intel Comet Lake: from 4.2.1.1 before 4.2.1.287; Phoenix SecureCore™ for Intel Tiger Lake: from 4.3.0.1 before 4.3.0.236; Phoenix SecureCore™ for Intel Jasper Lake: from 4.3.1.1 before 4.3.1.184; Phoenix SecureCore™ for Intel Alder Lake: from 4.4.0.1 before 4.4.0.269; Phoenix SecureCore™ for Intel Raptor Lake: from 4.5.0.1 before 4.5.0.218; Phoenix SecureCore™ for Intel Meteor Lake: from 4.5.1.1 before 4.5.1.15.	7.5	More Details
CVE-2024-32738	A sql injection vulnerability exists in CyberPower PowerPanel Enterprise prior to v2.8.3. An unauthenticated remote attacker can leak sensitive information via the "query_ptask_lean" function within MCUDBHelper.	7.5	More Details
CVE-2024-3372	Improper validation of certain metadata input may result in the server not correctly serialising BSON. This can be performed pre-authentication and may cause unexpected application behavior including unavailability of serverStatus responses. This issue affects MongoDB Server v7.0 versions prior to 7.0.6, MongoDB Server v6.0 versions prior to 6.0.14 and MongoDB Server v.5.0 versions prior to 5.0.25.	7.5	More Details
CVE-2024-4068	The NPM package `braces`, versions prior to 3.0.3, fails to limit the number of characters it can handle, which could lead to Memory Exhaustion. In `lib/parse.js,` if a malicious user sends "imbalanced braces" as input, the parsing will enter a loop, which will cause the program to start allocating heap memory without freeing it at any moment of the loop. Eventually, the JavaScript heap limit is reached, and the program will crash.	7.5	More Details
CVE-2024-34350	Next.js is a React framework that can provide building blocks to create web applications. Prior to 13.5.1, an inconsistent interpretation of a crafted HTTP request meant that requests are treated as both a single request, and two separate requests by Next.js, leading to desynchronized responses. This led to a response queue poisoning vulnerability in the affected Next.js versions. For a request to be exploitable, the affected route also had to be making use of the [rewrites](https://nextjs.org/docs/app/api-reference/next-config-js/rewrites) feature in Next.js. The vulnerability is resolved in Next.js `13.5.1` and newer.	7.5	More Details
CVE-2024-32712	Missing Authorization vulnerability in Podlove Podlove Podcast Publisher.This issue affects Podlove Podcast Publisher: from n/a through 4.0.14.	7.5	More Details
CVE-2024-34220	Sourcecodester Human Resource Management System 1.0 is vulnerable to SQL Injection via the 'leave' parameter.	7.5	More Details
CVE-2024-33865	An issue was discovered in linqi before 1.4.0.1 on Windows. There is an NTLM hash leak via the /api/Cdn/GetFile and /api/DocumentTemplate/{GUID] endpoints.	7.5	More Details
CVE-2024-32739	A sql injection vulnerability exists in CyberPower PowerPanel Enterprise prior to v2.8.3. An unauthenticated remote attacker can leak sensitive information via the "query_ptask_verbose" function within MCUDBHelper.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25581	When incoming DNS over HTTPS support is enabled using the nghttp2 provider, and queries are routed to a tcp-only or DNS over TLS backend, an attacker can trigger an assertion failure in DNSdist by sending a request for a zone transfer (AXFR or IXFR) over DNS over HTTPS, causing the process to stop and thus leading to a Denial of Service. DNS over HTTPS is not enabled by default, and backends are using plain DNS (Do53) by default.	7.5	More Details
CVE-2024-32991	Permission verification vulnerability in the wpa_supplicant module Impact: Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2024-3676	The Proofpoint Encryption endpoint of Proofpoint Enterprise Protection contains an Improper Input Validation vulnerability that allows an unauthenticated remote attacker with a specially crafted HTTP request to create additional Encryption user accounts under the attacker's control. These accounts are able to send spoofed email to any users within the domains configured by the Administrator.	7.5	More Details
CVE-2024-27790	Claris International has resolved an issue of potentially allowing unauthorized access to records stored in databases hosted on FileMaker Server. This issue has been fixed in FileMaker Server 20.3.2 by validating transactions before replying to client requests.	7.5	More Details
CVE-2024-30172	An issue was discovered in Bouncy Castle Java Cryptography APIs before 1.78. An Ed25519 verification code infinite loop can occur via a crafted signature and public key.	7.5	More Details
CVE-2024-27942	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected systems allow any unauthenticated client to disconnect any active user from the server. An attacker could use this vulnerability to prevent any user to perform actions in the system, causing a denial of service situation.	7.5	More Details
CVE-2024-34351	Next.js is a React framework that can provide building blocks to create web applications. A Server-Side Request Forgery (SSRF) vulnerability was identified in Next.js Server Actions. If the `Host` header is modified, and the below conditions are also met, an attacker may be able to make requests that appear to be originating from the Next.js application server itself. The required conditions are 1) Next.js is running in a self-hosted manner; 2) the Next.js application makes use of Server Actions; and 3) the Server Action performs a redirect to a relative path which starts with a `/`. This vulnerability was fixed in Next.js `14.1.1`.	7.5	More Details
CVE-2024-4791	A vulnerability classified as critical was found in Contemporary Control System BASrouter BACnet BASRT-B 2.7.2. This vulnerability affects unknown code of the component Application Protocol Data Unit. The manipulation leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-263890 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-2022-32508	An issue was discovered on certain Nuki Home Solutions devices. By sending a malformed HTTP verb, it is possible to force a reboot of the device. This affects Nuki Bridge v1 before 1.22.0 and v2 before 2.13.2.	7.5	More Details
CVE-2024-1598	Potential buffer overflow in unsafe UEFI variable handling in Phoenix SecureCore™ for Intel Gemini Lake.This issue affects: SecureCore™ for Intel Gemini Lake: from 4.1.0.1 before 4.1.0.567.	7.5	More Details
CVE-2024-30029	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	7.5	More Details
CVE-2024-23105	A Use Of Less Trusted Source [CWE-348] vulnerability in Fortinet FortiPortal version 7.0.0 through 7.0.6 and version 7.2.0 through 7.2.1 allows an unauthenticated attack to bypass IP protection through crafted HTTP or HTTPS packets.	7.5	More Details
CVE-2024-32992	Insufficient verification vulnerability in the baseband module Impact: Successful exploitation of this vulnerability will affect availability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34707	Nautobot is a Network Source of Truth and Network Automation Platform. A Nautobot user with admin privileges can modify the `BANNER_TOP`, `BANNER_BOTTOM`, and `BANNER_LOGIN` configuration settings via the `/admin/constance/config/` endpoint. Normally these settings are used to provide custom banner text at the top and bottom of all Nautobot web pages (or specifically on the login page in the case of `BANNER_LOGIN`) but it was reported that an admin user can make use of these settings to inject arbitrary HTML, potentially exposing Nautobot users to security issues such as cross-site scripting (stored XSS). The vulnerability is fixed in Nautobot 1.6.22 and 2.2.4.	7.5	More Details
CVE-2024-34244	libmodbus v3.1.10 is vulnerable to Buffer Overflow via the modbus_write_bits function. This issue can be triggered when the function is fed with specially crafted input, which leads to out-of-bounds read and can potentially cause a crash or other unintended behaviors.	7.5	More Details
CVE-2024-32612	HDF5 Library through 1.14.3 contains a heap-based buffer over-read in H5HL__fl_deserialize in H5HLcache.c, resulting in the corruption of the instruction pointer, a different vulnerability than CVE-2024-32613.	7.4	More Details
CVE-2024-32618	HDF5 Library through 1.14.3 contains a heap-based buffer overflow in H5T__get_native_type in H5Tnative.c, resulting in the corruption of the instruction pointer.	7.4	More Details
CVE-2024-32613	HDF5 Library through 1.14.3 contains a heap-based buffer over-read in the function H5HL__fl_deserialize in H5HLcache.c, a different vulnerability than CVE-2024-32612.	7.4	More Details
CVE-2024-32616	HDF5 Library through 1.14.3 contains a heap-based buffer over-read in H5O__dtype_encode_helper in H5Odtype.c.	7.4	More Details
CVE-2024-32624	HDF5 Library through 1.14.3 contains a heap-based buffer overflow in H5T__ref_mem_setnull in H5Tref.c (called from H5T__conv_ref in H5Tconv.c), resulting in the corruption of the instruction pointer.	7.4	More Details
CVE-2024-32620	HDF5 Library through 1.14.3 contains a heap-based buffer over-read in H5F_addr_decode_len in H5Fint.c, resulting in the corruption of the instruction pointer.	7.4	More Details
CVE-2024-32619	HDF5 Library through 1.14.3 contains a heap-based buffer overflow in H5T_copy_reopen in H5T.c, resulting in the corruption of the instruction pointer.	7.4	More Details
CVE-2024-32049	BIG-IP Next Central Manager (CM) may allow an unauthenticated, remote attacker to obtain the BIG-IP Next LTM/WAF instance credentials. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.4	More Details
CVE-2024-29160	HDF5 through 1.14.3 contains a heap buffer overflow in H5HG__cache_heap_deserialize, resulting in the corruption of the instruction pointer and causing denial of service or potential code execution.	7.4	More Details
CVE-2024-29165	HDF5 through 1.14.3 contains a buffer overflow in H5Z__filter_fletcher32, resulting in the corruption of the instruction pointer and causing denial of service or potential code execution.	7.4	More Details
CVE-2024-27394	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix Use-After-Free in tcp_ao_connect_init Since call_rcu, which is called in the hlist_for_each_entry_rcu traversal of tcp_ao_connect_init, is not part of the RCU read critical section, it is possible that the RCU grace period will pass during the traversal and the key will be free. To prevent this, it should be changed to hlist_for_each_entry_safe.	7.4	More Details
CVE-2024-28883	An origin validation vulnerability exists in BIG-IP APM browser network access VPN client for Windows, macOS and Linux which may allow an attacker to bypass F5 endpoint inspection. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.4	More Details
CVE-2024-29158	HDF5 through 1.14.3 contains a stack buffer overflow in H5FL_arr_malloc, resulting in the corruption of the instruction pointer and causing denial of service or potential code execution.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29162	HDF5 through 1.13.3 and/or 1.14.2 contains a stack buffer overflow in H5HG_read, resulting in denial of service or potential code execution.	7.4	More Details
CVE-2024-29163	HDF5 through 1.14.3 contains a heap buffer overflow in H5T__bit_find, resulting in the corruption of the instruction pointer and causing denial of service or potential code execution.	7.4	More Details
CVE-2024-1486	Elevation of privileges via misconfigured access control list in GE HealthCare ultrasound devices	7.4	More Details
CVE-2024-3460	In KioWare for Windows (versions all through 8.34) it is possible to exit this software and use other already opened applications utilizing a short time window before the forced automatic logout occurs. Then, by using some built-in function of these applications, one may launch any other programs. In order to exploit this vulnerability external applications must be left running when the KioWare software is launched. Additionally, an attacker must know the PIN set for this Kioware instance and also slow down the application with some specific task which extends the usable time window.	7.4	More Details
CVE-2024-25515	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the sys_file_storage_id parameter at /WorkFlow/wf_work_finish_file_down.aspx.	7.3	More Details
CVE-2024-32465	Git is a revision control system. The Git project recommends to avoid working in untrusted repositories, and instead to clone it first with `git clone --no-local` to obtain a clean copy. Git has specific protections to make that a safe operation even with an untrusted source repository, but vulnerabilities allow those protections to be bypassed. In the context of cloning local repositories owned by other users, this vulnerability has been covered in CVE-2024-32004. But there are circumstances where the fixes for CVE-2024-32004 are not enough: For example, when obtaining a `.zip` file containing a full copy of a Git repository, it should not be trusted by default to be safe, as e.g. hooks could be configured to run within the context of that repository. The problem has been patched in versions 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2, and 2.39.4. As a workaround, avoid using Git in repositories that have been obtained via archives from untrusted sources.	7.3	More Details
CVE-2024-34224	Cross Site Scripting vulnerability in /php-lms/classes/Users.php?f=save in Computer Laboratory Management System using PHP and MySQL 1.0 allow remote attackers to inject arbitrary web script or HTML via the firstname, middlename, lastname parameters.	7.3	More Details
CVE-2023-49781	NocoDB is software for building databases as spreadsheets. Prior to 0.202.9, a stored cross-site scripting vulnerability exists within the Formula virtual cell comments functionality. The nc-gui/components/virtual-cell/Formula.vue displays a v-html tag with the value of "urls" whose contents are processed by the function replaceUrlsWithLink(). This function recognizes the pattern URI::(XXX) and creates a hyperlink tag <a> with href=XXX. However, it leaves all the other contents outside of the pattern URI::(XXX) unchanged. This vulnerability is fixed in 0.202.9.	7.3	More Details
CVE-2024-34201	TOTOLINK CP450 v4.1.0cu.747_B20191224 was discovered to contain a stack buffer overflow vulnerability in the getSaveConfig function.	7.3	More Details
CVE-2024-34077	MantisBT (Mantis Bug Tracker) is an open source issue tracker. Insufficient access control in the registration and password reset process allows an attacker to reset another user's password and takeover their account, if the victim has an incomplete request pending. The exploit is only possible while the verification token is valid, i.e for 5 minutes after the confirmation URL sent by e-mail has been opened, and the user did not complete the process by updating their password. A brute-force attack calling account_update.php with increasing user IDs is possible. A successful takeover would grant the attacker full access to the compromised account, including sensitive information and functionalities associated with the account, the extent of which depends on its privileges and the data it has access to. Version 2.26.2 contains a patch for the issue. As a workaround, one may mitigate the risk by reducing the verification token's validity (change the value of the `TOKEN_EXPIRY_AUTHENTICATED` constant in `constants_inc.php`).	7.3	More Details
CVE-2024-34215	TOTOLINK CP450 v4.1.0cu.747_B20191224 was discovered to contain a stack buffer overflow vulnerability in the setUrlFilterRules function.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34212	TOTOLINK CP450 v4.1.0cu.747_B20191224 was discovered to contain a stack buffer overflow vulnerability in the CloudACMunualUpdate function.	7.3	More Details
CVE-2024-34205	TOTOLINK CP450 v4.1.0cu.747_B20191224 was discovered to contain a command injection vulnerability in the download_firmware function.	7.3	More Details
CVE-2024-31954	An issue was discovered in the installer in Samsung Portable SSD for T5 1.6.10 on Windows. Because it is possible to tamper with the directory and DLL files used during the installation process, an attacker can escalate privileges through arbitrary code execution. (An attacker must already have user privileges)	7.3	More Details
CVE-2023-46870	extcap/nrf_sniffer_ble.py, extcap/nrf_sniffer_ble.sh, extcap/SnifferAPI/*.py in Nordic Semiconductor nRF Sniffer for Bluetooth LE 3.0.0, 3.1.0, 4.0.0, 4.1.0, and 4.1.1 have set incorrect file permission, which allows attackers to do code execution via modified bash and python scripts.	7.3	More Details
CVE-2024-28279	Code-projects Computer Book Store 1.0 is vulnerable to SQL Injection via book.php?bookisbn=.	7.3	More Details
CVE-2024-34210	TOTOLINK outdoor CPE CP450 v4.1.0cu.747_B20191224 was discovered to contain a command injection vulnerability in the CloudACMunualUpdate function via the FileName parameter.	7.3	More Details
CVE-2024-4423	The access control in CemiPark software does not properly validate user-entered data, which allows the authentication bypass. An attacker who has network access to the login panel can log in with administrator rights to the application.This issue affects CemiPark software: 4.5, 4.7, 5.03 and potentially others. The vendor refused to provide the specific range of affected products.	7.2	More Details
CVE-2024-22264	VMware Avi Load Balancer contains a privilege escalation vulnerability. A malicious actor with admin privileges on VMware Avi Load Balancer can create, modify, execute and delete files as a root user on the host system.	7.2	More Details
CVE-2024-31477	Multiple authenticated command injection vulnerabilities exist in the command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2024-34338	Tenda O3V2 with firmware versions V1.0.0.10 and V1.0.0.12 was discovered to contain a Blind Command Injection via dest parameter in /goform/getTraceroute. This vulnerability allows attackers to execute arbitrary commands with root privileges. Authentication is required to exploit this vulnerability.	7.2	More Details
CVE-2021-22280	Improper DLL loading algorithms in B&R Automation Studio versions >=4.0 and <4.12 may allow an authenticated local attacker to execute code in the context of the product.	7.2	More Details
CVE-2024-27943	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected systems allow a privileged user to upload generic files to the root installation directory of the system. By replacing specific files, an attacker could tamper specific files or even achieve remote code execution.	7.2	More Details
CVE-2024-31476	Multiple authenticated command injection vulnerabilities exist in the command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2023-46714	A stack-based buffer overflow [CWE-121] vulnerability in Fortinet FortiOS version 7.2.1 through 7.2.6 and version 7.4.0 through 7.4.1 allows a privileged attacker over the administrative interface to execute arbitrary code or commands via crafted HTTP or HTTPs requests.	7.2	More Details
CVE-2024-2637	An Uncontrolled Search Path Element vulnerability in B&R Industrial Automation Scene Viewer, B&R Industrial Automation Automation Runtime, B&R Industrial Automation mapp Vision, B&R Industrial Automation mapp View, B&R Industrial Automation mapp Cockpit, B&R Industrial Automation mapp Safety, B&R Industrial Automation VC4 could allow an authenticated local attacker to execute malicious code by placing specially crafted files in the loading search path.This issue affects Scene Viewer: before 4.4.0; Automation Runtime: before J4.93; mapp Vision: before 5.26.1; mapp View: before 5.24.2; mapp Cockpit: before 5.24.2; mapp Safety: before 5.24.2; VC4: before 4.73.2.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27944	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected systems allow a privileged user to upload firmware files to the root installation directory of the system. By replacing specific files, an attacker could tamper specific files or even achieve remote code execution.	7.2	More Details
CVE-2024-33250	An issue in Open-Source Technology Committee SRS real-time video server RS/4.0.268(Leo) and SRS/4.0.195(Leo) allows a remote attacker to execute arbitrary code via a crafted request.	7.2	More Details
CVE-2024-27945	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The bulk import feature of the affected systems allow a privileged user to upload files to the root installation directory of the system. By replacing specific files, an attacker could tamper specific files or even achieve remote code execution.	7.2	More Details
CVE-2024-2290	The Advanced Ads plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.52.1 via deserialization of untrusted input in the 'placement_slug' parameter. This makes it possible for authenticated attackers to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	7.2	More Details
CVE-2024-31485	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V5.30), SICORE Base system (All versions < V1.3.0). The web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	7.2	More Details
CVE-2024-2662	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to command injection in all versions up to, and including, 1.5.102. This is due to insufficient filtering of template attributes during the creation of HTML for custom widgets This makes it possible for authenticated attackers, with administrator-level access and above, to execute arbitrary commands on the server.	7.2	More Details
CVE-2022-28132	The T-Soft E-Commerce 4 web application is susceptible to SQL injection (SQLi) attacks when authenticated as an admin or privileged user. This vulnerability allows attackers to access and manipulate the database through crafted requests. By exploiting this flaw, attackers can bypass authentication mechanisms, view sensitive information stored in the database, and potentially exfiltrate data.	7.2	More Details
CVE-2024-30044	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2024-34431	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP-etracker WP etracker allows Reflected XSS.This issue affects WP etracker: from n/a through 1.0.2.	7.1	More Details
CVE-2023-40720	An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiVoiceEntreprise version 7.0.0 through 7.0.1 and before 6.4.8 allows an authenticated attacker to read the SIP configuration of other users via crafted HTTP or HTTPS requests.	7.1	More Details
CVE-2024-22268	VMware Workstation and Fusion contain a heap buffer-overflow vulnerability in the Shader functionality. A malicious actor with non-administrative access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to create a denial of service condition.	7.1	More Details
CVE-2024-34818	Cross-Site Request Forgery (CSRF) vulnerability in WebinarPress.This issue affects WebinarPress: from n/a through 1.33.17.	7.1	More Details
CVE-2024-4747	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Propovoice Propovoice CRM allows Stored XSS.This issue affects Propovoice CRM: from n/a through 1.7.6.2.	7.1	More Details
CVE-2024-34231	A cross-site scripting (XSS) vulnerability in Sourcecodester Laboratory Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the System Short Name parameter.	7.1	More Details
CVE-2022-32505	An issue was discovered on certain Nuki Home Solutions devices. It is possible to send multiple BLE malformed packets to block some of the functionality and reboot the device. This affects Nuki Smart Lock 3.0 before 3.3.5 and Nuki Smart Lock 2.0 before 2.12.4.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52719	Privilege escalation vulnerability in the PMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	7.1	More Details
CVE-2024-23576	Security vulnerability in HCL Commerce 9.1.12 and 9.1.13 could allow denial of service, disclosure of user personal data, and performing of unauthorized administrative operations.	7.1	More Details
CVE-2022-32510	An issue was discovered on certain Nuki Home Solutions devices. The HTTP API exposed by a Bridge used an unencrypted channel to provide an administrative interface. A token can be easily eavesdropped by a malicious actor to impersonate a legitimate user and gain access to the full set of API endpoints. This affects Nuki Bridge v1 before 1.22.0 and v2 before 2.13.2.	7.1	More Details
CVE-2024-27825	A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions. This issue is fixed in macOS Sonoma 14.5. An app may be able to bypass certain Privacy preferences.	7.1	More Details
CVE-2024-32977	OctoPrint provides a web interface for controlling consumer 3D printers. OctoPrint versions up until and including 1.10.0 contain a vulnerability that allows an unauthenticated attacker to completely bypass the authentication if the `autologinLocal` option is enabled within `config.yaml`, even if they come from networks that are not configured as `localNetworks`, spoofing their IP via the `X-Forwarded-For` header. If autologin is not enabled, this vulnerability does not have any impact. The vulnerability has been patched in version 1.10.1. Until the patch has been applied, OctoPrint administrators who have autologin enabled on their instances should disable it and/or to make the instance inaccessible from potentially hostile networks like the internet.	7.1	More Details
CVE-2024-3903	The Add Custom CSS and JS WordPress plugin through 1.20 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in as author and above add Stored XSS payloads via a CSRF attack	7.1	More Details
CVE-2024-22269	VMware Workstation and Fusion contain an information disclosure vulnerability in the vbluetooth device. A malicious actor with local administrative privileges on a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual machine.	7.1	More Details
CVE-2024-22270	VMware Workstation and Fusion contain an information disclosure vulnerability in the Host Guest File Sharing (HGFS) functionality. A malicious actor with local administrative privileges on a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual machine.	7.1	More Details
CVE-2024-3951	PTC Codebeamer is vulnerable to a cross site scripting vulnerability that could allow an attacker to inject and execute malicious code.	7.1	More Details
CVE-2024-34553	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Select-Themes Stockholm Core allows Reflected XSS.This issue affects Stockholm Core: from n/a through 2.4.1.	7.1	More Details
CVE-2024-28134	An unauthenticated remote attacker can extract a session token with a MitM attack and gain web-based management access with the privileges of the currently logged in user due to cleartext transmission of sensitive information. No additional user interaction is required. The access is limited as only non-sensitive information can be obtained but the availability can be seriously affected.	7.0	More Details
CVE-2024-30033	Windows Search Service Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-27269	IBM QRadar SIEM 7.5 could allow a privileged user to configure user management that would disclose unintended sensitive information across tenants. IBM X-Force ID: 284575.	6.8	More Details
CVE-2024-27108	Non privileged access to critical file vulnerability in GE HealthCare EchoPAC products	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31488	An improper neutralization of inputs during web page generation vulnerability [CWE-79] in FortiNAC version 9.4.0 through 9.4.4, 9.2.0 through 9.2.8, 9.1.0 through 9.1.10, 8.8.0 through 8.8.11, 8.7.0 through 8.7.6, 7.2.0 through 7.2.3 may allow a remote authenticated attacker to perform stored and reflected cross site scripting (XSS) attack via crafted HTTP requests.	6.8	More Details
CVE-2024-30002	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-30021	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-30012	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-33612	An improper certificate validation vulnerability exists in BIG-IP Next Central Manager and may allow an attacker to impersonate an Instance Provider system. A successful exploit of this vulnerability can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.8	More Details
CVE-2024-29997	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-29999	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-30003	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-30004	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-32999	Cracking vulnerability in the OS security module Impact: Successful exploitation of this vulnerability will affect availability.	6.8	More Details
CVE-2024-29998	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-32874	Frigate is a network video recorder (NVR) with realtime local object detection for IP cameras. Below 0.13.2 Release, when uploading a file or retrieving the filename, a user may intentionally use a large Unicode filename which would lead to a application-level denial of service. This is due to no limitation set on the length of the filename and the costy use of the Unicode normalization with the form NFKD under the hood of `secure_filename()`.	6.8	More Details
CVE-2024-30005	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-4871	A vulnerability was found in Satellite. When running a remote execution job on a host, the host's SSH key is not being checked. When the key changes, the Satellite still connects it because it uses "-o StrictHostKeyChecking=no". This flaw can lead to a man-in-the-middle attack (MITM), denial of service, leaking of secrets the remote execution job contains, or other issues that may arise from the attacker's ability to forge an SSH key. This issue does not directly allow unauthorized remote execution on the Satellite, although it can leak secrets that may lead to it.	6.8	More Details
CVE-2024-30000	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30001	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2023-45583	A use of externally-controlled format string in Fortinet FortiProxy versions 7.2.0 through 7.2.5, 7.0.0 through 7.0.11, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6 FortiPAM versions 1.1.0, 1.0.0 through 1.0.3 FortiOS versions 7.4.0, 7.2.0 through 7.2.5, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15 FortiSwitchManager versions 7.2.0 through 7.2.2, 7.0.0 through 7.0.2 allows attacker to execute unauthorized code or commands via specially crafted cli commands and http requests.	6.7	More Details
CVE-2024-31952	An issue was discovered in Samsung Magician 8.0.0 on macOS. Because symlinks are used during the installation process, an attacker can escalate privileges via arbitrary file permission writes. (The attacker must already have user privileges, and an administrator password must be entered during the program installation stage for privilege escalation.)	6.7	More Details
CVE-2023-36640	A use of externally-controlled format string in Fortinet FortiProxy versions 7.2.0 through 7.2.4, 7.0.0 through 7.0.10, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiPAM versions 1.0.0 through 1.0.3, FortiOS versions 7.2.0, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.16 allows attacker to execute unauthorized code or commands via specially crafted commands	6.7	More Details
CVE-2024-31953	An issue was discovered in Samsung Magician 8.0.0 on macOS. Because it is possible to tamper with the directory and executable files used during the installation process, an attacker can escalate privileges through arbitrary code execution. (The attacker must already have user privileges, and an administrator password must be entered during the program installation stage for privilege escalation.)	6.7	More Details
CVE-2024-27460	A privilege escalation exists in the updater for Plantronics Hub 3.25.1 and below.	6.7	More Details
CVE-2024-25967	Dell PowerScale OneFS versions 8.2.x through 9.7.0.1 contains an execution with unnecessary privileges vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to escalation of privileges.	6.7	More Details
CVE-2024-27282	An issue was discovered in Ruby 3.x through 3.3.0. If attacker-supplied data is provided to the Ruby regex compiler, it is possible to extract arbitrary heap data relative to the start of the text, including pointers and sensitive strings. The fixed versions are 3.0.7, 3.1.5, 3.2.4, and 3.3.1.	6.6	More Details
CVE-2024-34081	MantisBT (Mantis Bug Tracker) is an open source issue tracker. Improper escaping of a custom field's name allows an attacker to inject HTML and, if CSP settings permit, achieve execution of arbitrary JavaScript when resolving or closing issues (`bug_change_status_page.php`) belonging to a project linking said custom field, viewing issues (`view_all_bug_page.php`) when the custom field is displayed as a column, or printing issues (`print_all_bug_page.php`) when the custom field is displayed as a column. Version 2.26.2 contains a patch for the issue. As a workaround, ensure Custom Field Names do not contain HTML tags.	6.6	More Details
CVE-2024-3788	Vulnerability in WBSAirback 21.02.04, which involves improper neutralisation of Server-Side Includes (SSI), through License (/admin/CDPUsers). Exploitation of this vulnerability could allow a remote user to execute arbitrary code.	6.6	More Details
CVE-2024-3787	Vulnerability in WBSAirback 21.02.04, which involves improper neutralisation of Server-Side Includes (SSI), through S3 disks (/admin/DeviceS3). Exploitation of this vulnerability could allow a remote user to execute arbitrary code.	6.6	More Details
CVE-2023-44247	A double free vulnerability [CWE-415] in Fortinet FortiOS before 7.0.0 may allow a privileged attacker to execute code or commands via crafted HTTP or HTTPs requests.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33495	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). The affected application does not properly limit the size of specific logs. This could allow an unauthenticated remote attacker to exhaust system resources by creating a great number of log entries which could potentially lead to a denial of service condition. A successful exploitation requires the attacker to have access to specific SIMATIC RTLS Locating Manager Clients in the deployment.	6.5	More Details
CVE-2024-33494	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected components do not properly authenticate heartbeat messages. This could allow an unauthenticated remote attacker to affected the availability of secondary RTLS systems configured using a TeeRevProxy service and potentially cause loss of data generated during the time the attack is ongoing.	6.5	More Details
CVE-2024-4039	The The Orders Tracking for WooCommerce plugin for WordPress for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.2.10. This is due to the plugin allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes. A partial patch was released in 1.2.10, and a complete patch was released in 1.2.11.	6.5	More Details
CVE-2024-33647	A vulnerability has been identified in Polarion ALM (All versions < V2404.0). The Apache Lucene based query engine in the affected application lacks proper access controls. This could allow an authenticated user to query items beyond the user's allowed projects.	6.5	More Details
CVE-2024-4823	Vulnerability in School ERP Pro+Responsive 1.0 that allows XSS via the index '/schoolerp/office_admin/' in the parameters es_bankacc, es_bank_name, es_bank_pin, es_checkno, es_teller_number, dc1 and dc2. An attacker could send a specially crafted JavaScript payload to an authenticated user and partially hijack their browser session.	6.5	More Details
CVE-2024-4822	Vulnerability in School ERP Pro+Responsive 1.0 that allows XSS via the username and password parameters in '/index.php'. This vulnerability allows an attacker to partially take control of the victim's browser session.	6.5	More Details
CVE-2024-4448	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'Dual Color Header', 'Event Calendar', & 'Advanced Data Table' widgets in all versions up to, and including, 5.9.19 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.5	More Details
CVE-2024-4038	The The Back In Stock Notifier for WooCommerce	WooCommerce Waitlist Pro plugin for WordPress for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 5.3.1. This is due to the plugin for WordPress allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	6.5	More Details
CVE-2024-4144	The Simple Basic Contact Form plugin for WordPress for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 20240502. This allows unauthenticated attackers to execute arbitrary shortcodes. The severity and exploitability depends on the functionality of other plugins installed in the environment.	6.5	More Details
CVE-2024-34432	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BetterAddons Better Elementor Addons better-elementor-addons allows Stored XSS.This issue affects Better Elementor Addons: from n/a through 1.4.4.	6.5	More Details
CVE-2024-34352	1Panel is an open source Linux server operation and maintenance management panel. Prior to v1.10.3-lts, there are many command injections in the project, and some of them are not well filtered, leading to arbitrary file writes, and ultimately leading to RCEs. The mirror configuration write symbol `>` can be used to achieve arbitrary file writing. This vulnerability is fixed in v1.10.3-lts.	6.5	More Details
CVE-2024-34191	htmly v2.9.6 was discovered to contain an arbitrary file deletion vulnerability via the delete_post() function at admin.php. This vulnerability allows attackers to delete arbitrary files via a crafted request.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4445	The WP Compress – Image Optimizer [All-In-One] plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the several functions in versions up to, and including, 6.20.01. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to edit plugin settings, including storing cross-site scripting, in multisite environments.	6.5	More Details
CVE-2024-25970	Dell PowerScale OneFS versions 8.2.x through 9.7.0.1 contains an improper input validation vulnerability. A low privileged remote attacker could potentially exploit this vulnerability, leading to loss of integrity.	6.5	More Details
CVE-2024-34699	GZ::CTF is a capture the flag platform. Prior to 0.20.1, unprivileged user can perform cross-site scripting attacks on other users by constructing malicious team names. This problem has been fixed in `v0.20.1`.	6.5	More Details
CVE-2024-1914	An attacker who successfully exploited these vulnerabilities could cause the robot to stop, make the robot controller inaccessible. The vulnerability could potentially be exploited to perform unauthorized actions by an attacker. This vulnerability arises under specific condition when specially crafted message is processed by the system. Below are reported vulnerabilities in the Robot Ware versions. * IRC5- RobotWare 6 < 6.15.06 except 6.10.10, and 6.13.07 * OmniCore- RobotWare 7 < 7.14	6.5	More Details
CVE-2024-34946	Tenda FH1206 V1.2.0.8(8155)_EN was discovered to contain a stack-based buffer overflow vulnerability via the page parameter at ip/goform/DhcpListClient.	6.5	More Details
CVE-2024-27946	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). Downloading files overwrites files with the same name in the installation directory of the affected systems. The filename for the target file can be specified, thus arbitrary files can be overwritten by an attacker with the required privileges.	6.5	More Details
CVE-2024-34445	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SKT Themes SKT Addons for Elementor allows Stored XSS.This issue affects SKT Addons for Elementor: from n/a through 1.8.	6.5	More Details
CVE-2024-34441	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bootstrapped Ventures Easy Affiliate Links allows Stored XSS.This issue affects Easy Affiliate Links: from n/a through 3.7.2.	6.5	More Details
CVE-2024-34436	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SKT Themes SKT Addons for Elementor allows Stored XSS.This issue affects SKT Addons for Elementor: from n/a through 1.8.	6.5	More Details
CVE-2024-3789	Uncontrolled resource consumption vulnerability in White Bear Solutions WBSAirback, version 21.02.04. This vulnerability could allow an attacker to send multiple command injection payloads to influence the amount of resources consumed.	6.5	More Details
CVE-2024-34421	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpsurface BlogLentor allows Stored XSS.This issue affects BlogLentor: from n/a through 1.0.8.	6.5	More Details
CVE-2024-34415	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThimPress Thim Elementor Kit allows Stored XSS.This issue affects Thim Elementor Kit: from n/a through 1.1.8.	6.5	More Details
CVE-2024-34354	CMSaaSStarter is a SaaS template/boilerplate built with SvelteKit, Tailwind, and Supabase. Any forks of the CMSaaSStarter template before commit 7904d416d2c72ec75f42fbf51e9e64fa74062ee6 are impacted. The issue is the user JWT Token is not verified on server session. You should take the patch 7904d416d2c72ec75f42fbf51e9e64fa74062ee6 into your fork.	6.5	More Details
CVE-2024-34712	Oceanic is a NodeJS library for interfacing with Discord. Prior to version 1.10.4, input to functions such as `Client.rest.channels.removeBan` is not url-encoded, resulting in specially crafted input such as `../../../channels/{id}` being normalized into the url `/api/v10/channels/{id}`, and deleting a channel rather than removing a ban. Version 1.10.4 fixes this issue. Some workarounds are available. One may sanitize user input, ensuring strings are valid for the purpose they are being used for. One may also encode input with `encodeURIComponent` before providing it to the library.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34687	SAP NetWeaver Application Server for ABAP and ABAP Platform do not sufficiently encode user controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker can control code that is executed within a user's browser, which could result in modification, deletion of data, including accessing or deleting files, or stealing session cookies which an attacker could use to hijack a user's session. Hence, this could have impact on Confidentiality, Integrity and Availability of the system.	6.5	More Details
CVE-2024-35167	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in EnvoThemes Envo's Elementor Templates & Widgets for WooCommerce allows Stored XSS.This issue affects Envo's Elementor Templates & Widgets for WooCommerce: from n/a through 1.4.8.	6.5	More Details
CVE-2023-46280	A vulnerability has been identified in Security Configuration Tool (SCT) (All versions), SIMATIC Automation Tool (All versions < V5.0 SP2), SIMATIC BATCH V9.1 (All versions < V9.1 SP2 Upd5), SIMATIC NET PC Software V16 (All versions < V16 Update 8), SIMATIC NET PC Software V17 (All versions), SIMATIC NET PC Software V18 (All versions < V18 SP1), SIMATIC NET PC Software V19 (All versions < V19 Update 2), SIMATIC PCS 7 V9.1 (All versions < V9.1 SP2 UC05), SIMATIC PDM V9.2 (All versions < V9.2 SP2 Upd3), SIMATIC Route Control V9.1 (All versions < V9.1 SP2 Upd3), SIMATIC S7-PCT (All versions < V3.5 SP3 Update 6), SIMATIC STEP 7 V5 (All versions < V5.7 SP3), SIMATIC WinCC OA V3.17 (All versions), SIMATIC WinCC OA V3.18 (All versions < V3.18 P025), SIMATIC WinCC OA V3.19 (All versions < V3.19 P010), SIMATIC WinCC Runtime Advanced (All versions < V17 Update 8), SIMATIC WinCC Runtime Professional V16 (All versions < V16 Update 6), SIMATIC WinCC Runtime Professional V17 (All versions < V17 Update 8), SIMATIC WinCC Runtime Professional V18 (All versions < V18 Update 4), SIMATIC WinCC Runtime Professional V19 (All versions < V19 Update 2), SIMATIC WinCC V7.4 (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 17), SIMATIC WinCC V8.0 (All versions < V8.0 Update 5), SINAMICS Startdrive (All versions < V19 SP1), SINEC NMS (All versions < V3.0), SINEC NMS (All versions < V3.0 SP1), SINUMERIK ONE virtual (All versions < V6.23), SINUMERIK PLC Programming Tool (All versions < V3.3.12), TIA Portal Cloud Connector (All versions < V2.0), Totally Integrated Automation Portal (TIA Portal) V15.1 (All versions), Totally Integrated Automation Portal (TIA Portal) V16 (All versions), Totally Integrated Automation Portal (TIA Portal) V17 (All versions < V17 Update 8), Totally Integrated Automation Portal (TIA Portal) V18 (All versions < V18 Update 4), Totally Integrated Automation Portal (TIA Portal) V19 (All versions < V19 Update 2). The affected applications contain an out of bounds read vulnerability. This could allow an attacker to cause a Blue Screen of Death (BSOD) crash of the underlying Windows kernel.	6.5	More Details
CVE-2024-34245	An arbitrary file read vulnerability in DedeCMS v5.7.114 allows authenticated attackers to read arbitrary files by specifying any path in makehtml_js_action.php.	6.5	More Details
CVE-2024-32730	SAP Enable Now Manager does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. On successful exploitation, the attacker with the role 'Learner' could gain access to other user's data in manager which will lead to a high impact to the confidentiality of the application.	6.5	More Details
CVE-2024-24908	Dell PowerProtect DM5500 version 5.15.0.0 and prior contain an Arbitrary File Delete via Path Traversal vulnerability. A remote attacker with high privileges could potentially exploit this vulnerability to deletion of arbitrary files stored on the server filesystem.	6.5	More Details
CVE-2024-33774	A buffer overflow vulnerability in /bin/boa on D-Link DIR-619L Rev.B 2.06B1 via formWlanSetup_Wizard allows remote authenticated users to trigger a denial of service (DoS) through the parameter "webpage."	6.5	More Details
CVE-2024-33773	A buffer overflow vulnerability in /bin/boa on D-Link DIR-619L Rev.B 2.06B1 via formWlanGuestSetup allows remote authenticated users to trigger a denial of service (DoS) through the parameter "webpage."	6.5	More Details
CVE-2024-33771	A buffer overflow vulnerability in /bin/boa on D-Link DIR-619L Rev.B 2.06B1 via goform/formWPS, allows remote authenticated users to trigger a denial of service (DoS) through the parameter "webpage."	6.5	More Details
CVE-2023-29881	phpok 6.4.003 is vulnerable to SQL injection in the function index_f() in phpok64/framework/api/call_control.php.	6.5	More Details
CVE-2023-37526	HCL DRYiCE Lucy (now AEX) is affected by a Cross Origin Resource Sharing (CORS) vulnerability. The mobile app is vulnerable to a CORS misconfiguration which could potentially allow unauthorized access to the application resources from any web domain and enable cache poisoning attacks.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33454	Buffer Overflow vulnerability in esp-idf v.5.1 allows a remote attacker to execute arbitrary code via a crafted script to the Bluetooth stack component.	6.5	More Details
CVE-2024-30054	Microsoft Power BI Client JavaScript SDK Information Disclosure Vulnerability	6.5	More Details
CVE-2023-43040	IBM Spectrum Fusion HCI 2.5.2 through 2.7.2 could allow an attacker to perform unauthorized actions in RGW for Ceph due to improper bucket access. IBM X-Force ID: 266807.	6.5	More Details
CVE-2023-50718	NocoDB is software for building databases as spreadsheets. Prior to version 0.202.10, an authenticated attacker with create access could conduct a SQL Injection attack on MySQL DB using unescaped `table_name`. This vulnerability may result in leakage of sensitive data in the database. Version 0.202.10 contains a patch for the issue.	6.5	More Details
CVE-2024-32776	Missing Authorization vulnerability in AppPresser Team AppPresser.This issue affects AppPresser: from n/a through 4.3.0.	6.5	More Details
CVE-2024-32717	Missing Authorization vulnerability in WPDeveloper SchedulePress.This issue affects SchedulePress: from n/a through 5.0.8.	6.5	More Details
CVE-2024-32761	Under certain conditions, a potential data leak may occur in the Traffic Management Microkernels (TMMs) of BIG-IP tenants running on VELOS and rSeries platforms. However, this issue cannot be exploited by an attacker because it is not consistently reproducible and is beyond an attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	6.5	More Details
CVE-2023-6682	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.9 prior to 16.9.7, starting from 16.10 prior to 16.10.5, and starting from 16.11 prior to 16.11.2. A problem with the processing logic for Discord Integrations Chat Messages can lead to a regular expression DoS attack on the server.	6.5	More Details
CVE-2024-32476	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. There is a Denial of Service (DoS) vulnerability via OOM using jq in ignoreDifferences. This vulnerability has been patched in version(s) 2.10.7, 2.9.12 and 2.8.16.	6.5	More Details
CVE-2023-6688	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.11 prior to 16.11.2. A problem with the processing logic for Google Chat Messages integration may lead to a regular expression DoS attack on the server.	6.5	More Details
CVE-2024-31460	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, some of the data stored in `automation_tree_rules.php` is not thoroughly checked and is used to concatenate the SQL statement in `create_all_header_nodes()` function from `lib/api_automation.php` , finally resulting in SQL injection. Using SQL based secondary injection technology, attackers can modify the contents of the Cacti database, and based on the modified content, it may be possible to achieve further impact, such as arbitrary file reading, and even remote code execution through arbitrary file writing. Version 1.2.27 contains a patch for the issue.	6.5	More Details
CVE-2024-0100	NVIDIA Triton Inference Server for Linux contains a vulnerability in the tracing API, where a user can corrupt system files. A successful exploit of this vulnerability might lead to denial of service and data tampering.	6.5	More Details
CVE-2024-30043	Microsoft SharePoint Server Information Disclosure Vulnerability	6.5	More Details
CVE-2024-30011	Windows Hyper-V Denial of Service Vulnerability	6.5	More Details
CVE-2024-2651	An issue has been discovered in GitLab CE/EE affecting all versions before 16.9.7, all versions starting from 16.10 before 16.10.5, all versions starting from 16.11 before 16.11.2. It was possible for an attacker to cause a denial of service using maliciously crafted markdown content.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2454	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.11 prior to 16.9.7, starting from 16.10 prior to 16.10.5, and starting from 16.11 prior to 16.11.2. The pins endpoint is susceptible to DoS through a crafted request.	6.5	More Details
CVE-2024-30036	Windows Deployment Services Information Disclosure Vulnerability	6.5	More Details
CVE-2024-27852	A privacy issue was addressed with improved client ID handling for alternative app marketplaces. This issue is fixed in iOS 17.5 and iPadOS 17.5. A maliciously crafted webpage may be able to distribute a script that tracks users on other webpages.	6.5	More Details
CVE-2024-33938	Missing Authorization vulnerability in codename065 Sliding Widgets allows Cross-Site Scripting (XSS).This issue affects Sliding Widgets: from n/a through 1.5.0.	6.5	More Details
CVE-2024-30053	Azure Migrate Cross-Site Scripting Vulnerability	6.5	More Details
CVE-2024-33951	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Adam DeHaven Perfect Pullquotes allows Stored XSS.This issue affects Perfect Pullquotes: from n/a through 1.7.5.	6.5	More Details
CVE-2024-34564	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LogicHunt Inc. Counter Up allows Stored XSS.This issue affects Counter Up: from n/a through 2.2.1.	6.5	More Details
CVE-2024-1930	No Limit on Number of Open Sessions / Bad Session Close Behaviour in dnf5daemon-server before 5.1.17 allows a malicious user to impact Availability via No Limit on Number of Open Sessions. There is no limit on how many sessions D-Bus clients may create using the `open_session()` D-Bus method. For each session a thread is created in dnf5daemon-server. This spends a couple of hundred megabytes of memory in the process. Further connections will become impossible, likely because no more threads can be spawned by the D-Bus service.	6.5	More Details
CVE-2024-22266	VMware Avi Load Balancer contains an information disclosure vulnerability. A malicious actor with access to the system logs can view cloud connection credentials in plaintext.	6.5	More Details
CVE-2024-34206	TOTOLINK outdoor CPE CP450 v4.1.0cu.747_B20191224 was discovered to contain a command injection vulnerability in the setWebWlanIdx function via the webWlanIdx parameter.	6.5	More Details
CVE-2024-34202	TOTOLINK CP450 v4.1.0cu.747_B20191224 was discovered to contain a stack buffer overflow vulnerability in the setMacFilterRules function.	6.5	More Details
CVE-2023-41651	Missing Authorization vulnerability in Multi-column Tag Map.This issue affects Multi-column Tag Map: from n/a through 17.0.26.	6.5	More Details
CVE-2024-34573	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pootlepress Pootle Pagebuilder – WordPress Page builder allows Stored XSS.This issue affects Pootle Pagebuilder – WordPress Page builder: from n/a through 5.7.1.	6.5	More Details
CVE-2024-34571	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGrill Himalayas allows Stored XSS.This issue affects Himalayas: from n/a through 1.3.0.	6.5	More Details
CVE-2024-33955	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Theme Freesia Freesia Empire allows Stored XSS.This issue affects Freesia Empire: from n/a through 1.4.1.	6.5	More Details
CVE-2024-34572	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemePrix Fancy Elementor Flipbox fancy-elementor-flipbox allows Stored XSS.This issue affects Fancy Elementor Flipbox: from n/a through 2.4.2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33952	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Justin Tadlock Unique allows Stored XSS.This issue affects Unique: from n/a through 0.3.0.	6.5	More Details
CVE-2024-34563	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GoldAddons Gold Addons for Elementor allows Stored XSS.This issue affects Gold Addons for Elementor: from n/a through 1.2.9.	6.5	More Details
CVE-2024-33954	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Atanas Yonkov Pliska allows Stored XSS.This issue affects Pliska: from n/a through 0.3.5.	6.5	More Details
CVE-2024-34562	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Moveaddons Move Addons for Elementor allows Stored XSS.This issue affects Move Addons for Elementor: from n/a through 1.3.0.	6.5	More Details
CVE-2024-30019	DHCP Server Service Denial of Service Vulnerability	6.5	More Details
CVE-2024-33953	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Matt van Andel Adventure Journal allows Stored XSS.This issue affects Adventure Journal: from n/a through 1.7.2.	6.5	More Details
CVE-2024-34414	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nobita allows Stored XSS.This issue affects raindrops: from n/a through 1.600.	6.5	More Details
CVE-2022-40218	Missing Authorization vulnerability in ThemeHunk Advance WordPress Search Plugin.This issue affects Advance WordPress Search Plugin: from n/a through 1.1.4.	6.5	More Details
CVE-2024-34566	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Johan van der Wijk Content Blocks (Custom Post Widget) allows Stored XSS.This issue affects Content Blocks (Custom Post Widget): from n/a through 3.3.0.	6.5	More Details
CVE-2024-3044	Unchecked script execution in Graphic on-click binding in affected LibreOffice versions allows an attacker to create a document which without prompt will execute scripts built-into LibreOffice on clicking a graphic. Such scripts were previously deemed trusted but are now deemed untrusted.	6.5	More Details
CVE-2024-34548	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themesgrove WidgetKit allows Stored XSS.This issue affects WidgetKit: from n/a through 2.4.8.	6.5	More Details
CVE-2024-34547	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noor alam Magical Addons For Elementor allows Stored XSS.This issue affects Magical Addons For Elementor: from n/a through 1.1.34.	6.5	More Details
CVE-2024-34569	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Katie Seaborn Zotpress allows Stored XSS.This issue affects Zotpress: from n/a through 7.3.9.	6.5	More Details
CVE-2024-4046	Cracking vulnerability in the OS security module Impact: Successful exploitation of this vulnerability will affect availability.	6.4	More Details
CVE-2024-4209	The Gutenberg Blocks with AI by Kadence WP – Page Builder Features plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the countdown timer in all versions up to, and including, 3.2.36 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4193	The Testimonial Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'testimonialcategory' shortcode in all versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4158	The Blocksy theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘tagName’ parameter in versions up to, and including, 2.0.42 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-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-2024-1166	The Image Hover Effects – Elementor Addon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Image Hover Effects Widget in all versions up to, and including, 1.4.1 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-2022-32506	An issue was discovered on certain Nuki Home Solutions devices. An attacker with physical access to the circuit board could use the SWD debug features to control the execution of code on the processor and debug the firmware, as well as read or alter the content of the internal and external flash memory. This affects Nuki Smart Lock 3.0 before 3.3.5, Nuki Smart Lock 2.0 before 2.12.4, as well as Nuki Bridge v1 before 1.22.0 and v2 before 2.13.2.	6.4	More Details
CVE-2024-3990	The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Tooltip & Popover Widget in all versions up to, and including, 2.5.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3989	The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Gallery Justify Widget in all versions up to, and including, 2.5.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3974	The BuddyPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘user_name’ parameter in versions up to, and including, 12.4.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-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-2024-3494	The Mesmerize Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mesmerize_contact_form' shortcode in all versions up to, and including, 1.6.148 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3952	The Advanced Ads – Ad Manager & AdSense plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Advanced Ad widget in all versions up to, and including, 1.52.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3923	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the link_target parameter in all versions up to, and including, 2.8.1.1 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-2024-3831	The Enter Addons – Ultimate Template Builder for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Heading widget in all versions up to, and including, 2.1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-24787	On Darwin, building a Go module which contains CGO can trigger arbitrary code execution when using the Apple version of ld, due to usage of the -lto_library flag in a "#cgo LDFLAGS" directive.	6.4	More Details
CVE-2024-4854	MONGO and ZigBee TLV dissector infinite loops in Wireshark 4.2.0 to 4.2.4, 4.0.0 to 4.0.14, and 3.6.0 to 3.6.22 allow denial of service via packet injection or crafted capture file	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0445	The The Plus Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's element attributes in all versions up to, and including, 5.4.2 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. CVE-2024-34373 is likely a duplicate of this issue.	6.4	More Details
CVE-2024-4567	The Themify Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's themify_button shortcode in all versions up to, and including, 2.0.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4275	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Interactive Circle widget in all versions up to, and including, 5.9.19 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4630	The Starter Templates — Elementor, WordPress & Beaver Builder Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘custom_upload_mimes’ function in versions up to, and including, 4.2.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-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-2024-4490	The Elegant Themes Divi theme, Extra theme, and Divi Page Builder plugin for WordPress are vulnerable to DOM-Based Stored Cross-Site Scripting via the ‘title’ parameter in versions up to, and including, 4.25.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-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-2024-4487	The Blocksy Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG uploads in versions up to, and including, 2.0.45 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-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-2024-4481	The Gutenberg Blocks with AI by Kadence WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' attribute of the plugin's blocks in all versions up to, and including, 3.2.36 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4449	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'Fancy Text', 'Filter Gallery', 'Sticky Video', 'Content Ticker', 'Woo Product Gallery', & 'Twitter Feed' widgets in all versions up to, and including, 5.9.19 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4446	The Content Views – Post Grid & Filter, Recent Posts, Category Posts, & More (Gutenberg Blocks and Shortcode) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘pagingType’ parameter in all versions up to, and including, 3.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4430	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the photo widget crop attribute in all versions up to, and including, 2.8.1.2 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-2024-4411	The Mihdan: Yandex Turbo Feed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.6.5.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4398	The HTML5 Audio Player- Best WordPress Audio Player Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 2.2.19 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4386	The Gallery Block (Meow Gallery) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘data_atts’ parameter in versions up to, and including, 5.1.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-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-2024-4574	The Graphina – Elementor Charts and Graphs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 1.8.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4383	The Simple Membership plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'swpm_paypal_subscription_cancel_link' shortcode in all versions up to, and including, 4.4.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4339	The Prime Slider – Addons For Elementor (Revolution of a slider, Hero Slider, Ecommerce Slider) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the General widget in all versions up to, and including, 3.14.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4335	The Rank Math SEO with AI Best SEO Tools plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘textAlign’ parameter in versions up to, and including, 1.0.217 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-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-2024-4281	The Link Library plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'link-library' shortcode in all versions up to, and including, 7.6.11 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4329	The Thim Elementor Kit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘id’ parameter in all versions up to, and including, 1.1.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4316	The EmbedPress – Embed PDF, Google Docs, Vimeo, Wistia, Embed YouTube Videos, Audios, Maps & Embed Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘id’ parameter in all versions up to, and including, 3.9.16 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3680	The Enter Addons – Ultimate Template Builder for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Animation Title widget's img tag in all versions up to, and including, 2.1.5 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-2024-4277	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘layout_html’ parameter in all versions up to, and including, 4.2.6.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4107	The Elementor Website Builder – More than Just a Page Builder Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the several parameters in versions up to, and including, 3.21.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-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 Number	Description	Base Score	Reference
CVE-2024-3595	The Pure Chat – Live Chat Plugin & More! plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the purechatwid and purechatwname parameter in all versions up to, and including, 2.22 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber access or above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2785	The The Plus Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Age Gate widget in all versions up to, and including, 5.4.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4624	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugins for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘eael_ext_toc_title_tag’ parameter in versions up to, and including, 5.9.20 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-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-2024-4473	The Sydney Toolbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the "aThemes: Portfolio" widget in all versions up to, and including, 1.31 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4440	The 140+ Widgets	Best Addons For Elementor – FREE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 1.4.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4392	The Jetpack – WP Security, Backup, Speed, & Growth plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpvideo shortcode in all versions up to, and including, 13.3.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4333	The Sina Extension for Elementor (Slider, Gallery, Form, Modal, Data Table, Tab, Particle, Free Elementor Widgets & Elementor Templates) plugin for WordPress is vulnerable to DOM-Based Cross-Site Scripting via several parameters in versions up to, and including, 3.5.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-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-2024-2923	The Magical Addons For Elementor (Header Footer Builder, Free Elementor Widgets, Elementor Templates Library) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's text effect widget in all versions up to, and including, 1.1.37 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4666	The Borderless – Widgets, Elements, Templates and Toolkit for Elementor & Gutenberg plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 1.5.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5052	vulnerability in Uniform Server Zero, version 10.2.5, consisting of an XSS through the /us_extra/phpinfo.php page. This vulnerability could allow a remote user to send a specially crafted query to an authenticated user and partially take over their session details.	6.3	More Details
CVE-2024-4800	A vulnerability has been found in Kashipara College Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file submit_student.php. The manipulation of the argument date_of_birth 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-263920.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33497	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected SIMATIC RTLS Locating Manager Track Viewer Client do not properly protect credentials that are used to authenticate to the server. This could allow an authenticated local attacker to extract the credentials and use them to escalate their access rights from the Manager to the Systemadministrator role.	6.3	More Details
CVE-2024-33496	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected SIMATIC RTLS Locating Manager Report Clients do not properly protect credentials that are used to authenticate to the server. This could allow an authenticated local attacker to extract the credentials and use them to escalate their access rights from the Manager to the Systemadministrator role.	6.3	More Details
CVE-2024-4805	A vulnerability classified as critical has been found in Kashipara College Management System 1.0. This affects an unknown part of the file edit_faculty.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-263925 was assigned to this vulnerability.	6.3	More Details
CVE-2024-4653	A vulnerability was found in BlueNet Technology Clinical Browsing System 1.2.1 and classified as critical. Affected by this issue is some unknown functionality of the file /xds/outIndex.php. The manipulation of the argument name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-263498 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-4654	A vulnerability was found in BlueNet Technology Clinical Browsing System 1.2.1. It has been classified as critical. This affects an unknown part of the file /xds/cloudInterface.php. The manipulation of the argument INSTI_CODE 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-263499.	6.3	More Details
CVE-2024-4803	A vulnerability was found in Kashipara College Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file submit_admin.php. The manipulation of the argument phone 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-263923.	6.3	More Details
CVE-2024-4802	A vulnerability was found in Kashipara College Management System 1.0. It has been classified as critical. Affected is an unknown function of the file submit_extracurricular_activity.php. The manipulation of the argument activity_datetime 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-263922 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-4801	A vulnerability was found in Kashipara College Management System 1.0 and classified as critical. This issue affects some unknown processing of the file submit_new_faculty.php. The manipulation of the argument address 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-263921 was assigned to this vulnerability.	6.3	More Details
CVE-2024-35012	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/infoType_deal.php?mudi=add&nohrefStr=close.	6.3	More Details
CVE-2024-4799	A vulnerability, which was classified as critical, was found in Kashipara College Management System 1.0. This affects an unknown part of the file view_each_faculty.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-263919.	6.3	More Details
CVE-2024-4807	A vulnerability, which was classified as critical, has been found in Kashipara College Management System 1.0. This issue affects some unknown processing of the file delete_user.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 associated identifier of this vulnerability is VDB-263927.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4798	A vulnerability, which was classified as critical, has been found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this issue is some unknown functionality of the file /admin/maintenance/manage_brand.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-263918 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-30045	.NET and Visual Studio Remote Code Execution Vulnerability	6.3	More Details
CVE-2024-4796	A vulnerability was found in Campcodes Online Laundry Management System 1.0. It has been classified as critical. This affects an unknown part of the file /manage_inv.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-263895.	6.3	More Details
CVE-2024-4795	A vulnerability was found in Campcodes Online Laundry Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /manage_user.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-263894 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-4794	A vulnerability has been found in Campcodes Online Laundry Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /manage_receiving.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-263893 was assigned to this vulnerability.	6.3	More Details
CVE-2024-4793	A vulnerability, which was classified as critical, was found in Campcodes Online Laundry Management System 1.0. Affected is an unknown function of the file /manage_laundry.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. The identifier of this vulnerability is VDB-263892.	6.3	More Details
CVE-2024-4792	A vulnerability, which was classified as critical, has been found in Campcodes Online Laundry Management System 1.0. This issue affects some unknown processing of the file /admin_class.php. The manipulation of the argument id/delete_category/delete_inv/delete_laundry/delete_supply/delete_user/login/save_inv/save_user 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-263891.	6.3	More Details
CVE-2022-32502	An issue was discovered on certain Nuki Home Solutions devices. There is a buffer overflow over the encrypted token parsing logic in the HTTP service that allows remote code execution. This affects Nuki Bridge v1 before 1.22.0 and v2 before 2.13.2.	6.3	More Details
CVE-2024-34695	WOWS Karma is a reputation system for Wargaming's World of Warships. A user is able to click multiple times on "create" on a post creation prompt before the modal closes, which triggers sending several post creation API requests at once. Due to timing, sending multiple posts simultaneously requests bypasses the cooldown validation, however are not refreshing a user's metrics more than once, due to concurrent karma updates. This issue is fixed in 0.17.4.1.	6.3	More Details
CVE-2024-4806	A vulnerability classified as critical was found in Kashipara College Management System 1.0. This vulnerability affects unknown code of the file each_extracurricula_activities.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-263926 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-4804	A vulnerability was found in Kashipara College Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file edit_user.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-263924.	6.3	More Details
CVE-2024-30208	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). The "DBTest" tool of SIMATIC RTLS Locating Manager does not properly enforce access restriction. This could allow an authenticated local attacker to extract sensitive information from memory.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4820	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /classes/SystemSettings.php?f=update_settings. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-263941 was assigned to this vulnerability.	6.3	More Details
CVE-2024-4817	A vulnerability has been found in Campcodes Online Laundry Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file manage_user.php of the component HTTP Request Parameter Handler. The manipulation of the argument id leads to improper control of resource identifiers. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-263938 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-4808	A vulnerability, which was classified as critical, was found in Kashipara College Management System 1.0. Affected is an unknown function of the file delete_faculty.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. The identifier of this vulnerability is VDB-263928.	6.3	More Details
CVE-2024-4816	A vulnerability, which was classified as critical, was found in Ruijie RG-UAC up to 20240506. This affects an unknown part of the file /view/networkConfig/GRE/gre_add_commit.php. The manipulation of the argument name/remote/local/IP 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-263937 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-2024-4809	A vulnerability has been found in SourceCodester Open Source Clinic Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file setting.php. The manipulation of the argument logo leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-263929 was assigned to this vulnerability.	6.3	More Details
CVE-2024-4699	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DAR-8000-10 up to 20230922. This issue affects some unknown processing of the file /importhtml.php. The manipulation of the argument sql leads to deserialization. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-263747. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2024-4815	A vulnerability, which was classified as critical, has been found in Ruijie RG-UAC up to 20240506. Affected by this issue is some unknown functionality of the file /view/bugSolve/viewData/detail.php. The manipulation of the argument filename 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-263936. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-4813	A vulnerability classified as critical has been found in Ruijie RG-UAC up to 20240506. Affected is an unknown function of the file /view/networkConfig/physicalInterface/interface_commit.php. The manipulation of the argument name leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. VDB-263934 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-2024-4814	A vulnerability classified as critical was found in Ruijie RG-UAC up to 20240506. Affected by this vulnerability is an unknown functionality of the file /view/networkConfig/RouteConfig/StaticRoute/static_route_edit_commit.php. The manipulation of the argument oldipmask/oldgateway 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-263935. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-32996	Privilege escalation vulnerability in the account module Impact: Successful exploitation of this vulnerability will affect availability.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4418	A race condition leading to a stack use-after-free flaw was found in libvirt. Due to a bad assumption in the virNetClientIOEventLoop() method, the `data` pointer to a stack-allocated virNetClientIOEventData structure ended up being used in the virNetClientIOEventFD callback while the data pointer's stack frame was concurrently being "freed" when returning from virNetClientIOEventLoop(). The 'virtproxyd' daemon can be used to trigger requests. If libvirt is configured with fine-grained access control, this issue, in theory, allows a user to escape their otherwise limited access. This flaw allows a local, unprivileged user to access virtproxyd without authenticating. Remote users would need to authenticate before they could access it.	6.2	More Details
CVE-2023-52721	The WindowManager module has a vulnerability in permission control. Impact: Successful exploitation of this vulnerability may affect confidentiality.	6.2	More Details
CVE-2024-25969	Dell PowerScale OneFS versions 8.2.x through 9.7.0.1 contains an allocation of resources without limits or throttling vulnerability. A local unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service.	6.2	More Details
CVE-2024-31803	Buffer Overflow vulnerability in emp-ot v.0.2.4 allows a remote attacker to execute arbitrary code via the FerretCOT<T>::read_pre_data128_from_file function.	6.2	More Details
CVE-2024-3461	KioWare for Windows (versions all through 8.35) allows to brute force the PIN number, which protects the application from being closed, as there are no mechanisms preventing a user from excessively guessing the number.	6.2	More Details
CVE-2024-32995	Denial of service (DoS) vulnerability in the AMS module Impact: Successful exploitation of this vulnerability will affect availability.	6.2	More Details
CVE-2024-22345	IBM TXSeries for Multiplatforms 8.2 transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. IBM X-Force ID: 280192.	6.2	More Details
CVE-2024-1629	Path traversal vulnerability in “deleteFiles” function of Common Service Desktop, a GE HealthCare ultrasound device component	6.2	More Details
CVE-2024-26367	Cross Site Scripting vulnerability in Evertz microsystems MViP-II Firmware 8.6.5, XPS-EDGE-* Build 1467, evEDGE-EO-* Build 0029, MMA10G-* Build 0498, 570IPG-X19-10G Build 0691 allows a remote attacker to execute arbitrary code via a crafted payload to the login parameters.	6.1	More Details
CVE-2024-32733	Due to missing input validation and output encoding of untrusted data, SAP NetWeaver Application Server ABAP and ABAP Platform allows an unauthenticated attacker to inject malicious JavaScript code into the dynamically crafted web page. On successful exploitation the attacker can access or modify sensitive information with no impact on availability of the application	6.1	More Details
CVE-2024-30059	Microsoft Intune for Android Mobile Application Management Tampering Vulnerability	6.1	More Details
CVE-2024-34074	Frappe is a full-stack web application framework. Prior to 15.26.0 and 14.74.0, the login page accepts redirect argument and it allowed redirect to untrusted external URIs. This behaviour can be used by malicious actors for phishing. This vulnerability is fixed in 15.26.0 and 14.74.0.	6.1	More Details
CVE-2024-3590	The LetterPress WordPress plugin through 1.2.2 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks, such as delete arbitrary subscribers	6.1	More Details
CVE-2024-32990	Permission verification vulnerability in the system sharing pop-up module Impact: Successful exploitation of this vulnerability will affect availability.	6.1	More Details
CVE-2024-25965	Dell PowerScale OneFS versions 8.2.x through 9.7.0.2 contains an external control of file name or path vulnerability. A local high privilege attacker could potentially exploit this vulnerability, leading to denial of service.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33002	Document Service handler (obsolete) in Data Provisioning Service does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability with low impact on Confidentiality and Integrity of the application.	6.1	More Details
CVE-2024-28276	Sourcecodester School Task Manager 1.0 is vulnerable to Cross Site Scripting (XSS) via add-task.php?task_name=.	6.1	More Details
CVE-2024-34225	Cross Site Scripting vulnerability in php-lms/admin/?page=system_info in Computer Laboratory Management System using PHP and MySQL 1.0 allow remote attackers to inject arbitrary web script or HTML via the name, shortname parameters.	6.1	More Details
CVE-2024-33604	A reflected cross-site scripting (XSS) vulnerability exist in undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	6.1	More Details
CVE-2024-34255	jizhicms v2.5.1 contains a Cross-Site Scripting(XSS) vulnerability in the message function.	6.1	More Details
CVE-2024-3547	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'google_connect_error' parameter in all versions up to, and including, 1.5.102 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-2024-3579	Open-source project Online Shopping System Advanced is vulnerable to Reflected Cross-Site Scripting (XSS). An attacker might trick somebody into using a crafted URL, which will cause a script to be run in user's browser.	6.1	More Details
CVE-2024-4041	The Yoast SEO plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via URLs in all versions up to, and including, 22.5 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-2024-4768	A bug in popup notifications' interaction with WebAuthn made it easier for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 126, Firefox ESR < 115.11, and Thunderbird < 115.11.	6.1	More Details
CVE-2024-22910	Cross Site Scripting (XSS) vulnerability in CrushFTP v.10.6.0 and v.10.5.5 allows an attacker to execute arbitrary code via a crafted payload.	6.1	More Details
CVE-2024-4150	The Simple Basic Contact Form plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘scf_email’ parameter in versions up to, and including, 20221201 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-2024-34230	A cross-site scripting (XSS) vulnerability in Sourcecodester Laboratory Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the System Information parameter.	6.1	More Details
CVE-2024-4104	The ADFO – Custom data in admin dashboard plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'dbp_id' parameter in all versions up to, and including, 1.9.0 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-2024-22344	IBM TXSeries for Multiplatforms 8.2 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 280191.	6.1	More Details
CVE-2024-30268	Cacti provides an operational monitoring and fault management framework. A reflected cross-site scripting vulnerability on the 1.3.x DEV branch allows attackers to obtain cookies of administrator and other users and fake their login using obtained cookies. This issue is fixed in commit a38b9046e9772612fda847b46308f9391a49891e.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25662	Oxygen XML Web Author v26.0.0 and older and Oxygen Content Fusion v6.1 and older are vulnerable to Cross-Site Scripting (XSS) for malicious URLs.	6.1	More Details
CVE-2024-32349	TOTOLINK X5000R V9.1.0cu.2350_B20230313 was discovered to contain an authenticated remote command execution (RCE) vulnerability via the "mtu" parameters in the "cstecgi.cgi" binary.	6.0	More Details
CVE-2024-32354	TOTOLINK X5000R V9.1.0cu.2350_B20230313 was discovered to contain a command injection vulnerability via the 'timeout' parameter in the setSSServer function at /cgi-bin/cstecgi.cgi.	6.0	More Details
CVE-2024-34422	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in trinhtuantai Viet Affiliate Link allows Stored XSS.This issue affects Viet Affiliate Link: from n/a through 1.2.	5.9	More Details
CVE-2024-34430	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rashed Latif TT Custom Post Type Creator allows Stored XSS.This issue affects TT Custom Post Type Creator: from n/a through 1.0.	5.9	More Details
CVE-2024-30171	An issue was discovered in Bouncy Castle Java TLS API and JSSE Provider before 1.78. Timing-based leakage may occur in RSA based handshakes because of exception processing.	5.9	More Details
CVE-2024-33950	Administrator Cross Site Scripting (XSS) in Archives Calendar Widget <= 1.0.15 versions.	5.9	More Details
CVE-2024-28889	When an SSL profile with alert timeout is configured with a non-default value on a virtual server, undisclosed traffic along with conditions beyond the attacker's control can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.9	More Details
CVE-2024-4769	When importing resources using Web Workers, error messages would distinguish the difference between `application/javascript` responses and non-script responses. This could have been abused to learn information cross-origin. This vulnerability affects Firefox < 126, Firefox ESR < 115.11, and Thunderbird < 115.11.	5.9	More Details
CVE-2024-4772	An HTTP digest authentication nonce value was generated using `rand()` which could lead to predictable values. This vulnerability affects Firefox < 126.	5.9	More Details
CVE-2024-4775	An iterator stop condition was missing when handling WASM code in the built-in profiler, potentially leading to invalid memory access and undefined behavior. *Note:* This issue only affects the application when the profiler is running. This vulnerability affects Firefox < 126.	5.9	More Details
CVE-2024-34424	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in iePlexus Featured Content Gallery allows Stored XSS.This issue affects Featured Content Gallery: from n/a through 3.2.0.	5.9	More Details
CVE-2024-2749	The VikBooking Hotel Booking Engine & PMS WordPress plugin before 1.6.8's access control mechanism fails to properly restrict access to its settings, permitting any users that can access a menu to manipulate requests and perform unauthorized actions such as editing, renaming or deleting (categories for example) despite initial settings prohibiting such access. This vulnerability resembles broken access control, enabling unauthorized users to modify critical VikBooking Hotel Booking Engine & PMS WordPress plugin before 1.6.8 configurations.	5.9	More Details
CVE-2024-33864	An issue was discovered in linqi before 1.4.0.1 on Windows. There is SSRF via Document template generation; i.e., via remote images in process creation, file inclusion, and PDF document generation via malicious JavaScript.	5.9	More Details
CVE-2024-35169	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AREOI All Bootstrap Blocks allows Stored XSS.This issue affects All Bootstrap Blocks: from n/a through 1.3.15.	5.9	More Details
CVE-2024-34570	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xpro Xpro Elementor Addons allows Stored XSS.This issue affects Xpro Elementor Addons: from n/a through 1.4.3.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34222	Sourcecodester Human Resource Management System 1.0 is vulnerable to SQL Injection via the searccountry parameter.	5.9	More Details
CVE-2024-34561	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Creative interactive media 3D FlipBook, PDF Viewer, PDF Embedder – Real 3D FlipBook WordPress Plugin allows Stored XSS.This issue affects 3D FlipBook, PDF Viewer, PDF Embedder – Real 3D FlipBook WordPress Plugin: from n/a through 3.71.	5.9	More Details
CVE-2024-34560	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GOMO gee Search Plus allows Stored XSS.This issue affects gee Search Plus: from n/a through 1.4.4.	5.9	More Details
CVE-2024-34558	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in realmag777 WOLF allows Stored XSS.This issue affects WOLF: from n/a through 1.0.8.2.	5.9	More Details
CVE-2024-34429	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Orchestrated Corona Virus (COVID-19) Banner & Live Data allows Stored XSS.This issue affects Corona Virus (COVID-19) Banner & Live Data: from n/a through 1.8.0.2.	5.9	More Details
CVE-2024-34428	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Harknell AWSOM News Announcement allows Stored XSS.This issue affects AWSOM News Announcement: from n/a through 1.6.0.	5.9	More Details
CVE-2024-34546	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HabibCoder Sticky Social Link allows Stored XSS.This issue affects Sticky Social Link: from n/a through 1.0.0.	5.9	More Details
CVE-2024-35170	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hidden Depth Sticky banner allows Stored XSS.This issue affects Sticky banner: from n/a through 1.2.0.	5.9	More Details
CVE-2024-34426	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Benoti Brozzme Scroll Top allows Stored XSS.This issue affects Brozzme Scroll Top: from n/a through 1.8.5.	5.9	More Details
CVE-2024-34701	CreateWiki is Miraheze's MediaWiki extension for requesting & creating wikis. It is possible for users to be considered as the requester of a specific wiki request if their local user ID on any wiki in a wiki farm matches the local ID of the requester at the wiki where the wiki request was made. This allows them to go to that request entry's on Special:RequestWikiQueue on the wiki where their local user ID matches and take any actions that the wiki requester is allowed to take from there. Commit 02e0f298f8d35155c39aa74193cb7b867432c5b8 fixes the issue. Important note about the fix: This vulnerability has been fixed by disabling access to the REST API and special pages outside of the wiki configured as the "global wiki" in `$wgCreateWikiGlobalWiki` in a user's MediaWiki settings. As a workaround, it is possible to disable the special pages outside of one's own global wiki by doing something similar to `miraheze/mw-config` commit e5664995fbb8644f9a80b450b4326194f20f9ddc that is adapted to one's own setup. As for the REST API, before the fix, there wasn't any REST endpoint that allowed one to make writes. Regardless, it is possible to also disable it outside of the global wiki by using `$wgCreateWikiDisableRESTAPI` and `$wgConf` in the configuration for one's own wiki farm..	5.9	More Details
CVE-2024-25968	Dell PowerScale OneFS versions 8.2.x through 9.7.0.2 contains a use of a broken or risky cryptographic algorithm vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to information disclosure.	5.9	More Details
CVE-2024-34704	era-compiler-solidity is the ZKsync compiler for Solidity. The problem occurred during instruction selection in the `DAGCombine` phase while visiting the XOR operation. The issue arises when attempting to fold the expression `!(x cc y)` into `(x !cc y)`. To perform this transformation, the second operand of XOR should be a constant representing the true value. However, it was incorrectly assumed that -1 represents the true value, when in fact, 1 is the correct representation, so this transformation for this case should be skipped. This vulnerability is fixed in 1.4.1.	5.9	More Details
CVE-2024-34420	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in talspotim Comments Evolved for WordPress allows Stored XSS.This issue affects Comments Evolved for WordPress: from n/a through 1.6.3.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32998	NULL pointer access vulnerability in the clock module Impact: Successful exploitation of this vulnerability will affect availability.	5.9	More Details
CVE-2023-38264	The IBM SDK, Java Technology Edition's Object Request Broker (ORB) 7.1.0.0 through 7.1.5.21 and 8.0.0.0 through 8.0.8.21 is vulnerable to a denial of service attack in some circumstances due to improper enforcement of the JEP 290 MaxRef and MaxDepth deserialization filters. IBM X-Force ID: 260578.	5.9	More Details
CVE-2024-34419	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nathan Vonnahme Configure Login Timeout allows Stored XSS.This issue affects Configure Login Timeout: from n/a through 1.0.	5.9	More Details
CVE-2024-34418	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tech9logy Creators WPCS (WordPress Custom Search) allows Stored XSS.This issue affects WPCS (WordPress Custom Search): from n/a through 1.1.	5.9	More Details
CVE-2024-34417	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Toidicode.Com (thanhtaivtt) Viet Nam Affiliate allows Stored XSS.This issue affects Viet Nam Affiliate: from n/a through 1.0.0.	5.9	More Details
CVE-2024-34565	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Debug Info allows Stored XSS.This issue affects Debug Info: from n/a through 1.3.10.	5.9	More Details
CVE-2024-34811	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VeronaLabs WP SMS allows Stored XSS.This issue affects WP SMS: from n/a through 6.5.1.	5.9	More Details
CVE-2024-34437	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 10Web Form Builder Team Form Maker by 10Web allows Stored XSS.This issue affects Form Maker by 10Web: from n/a through 1.15.24.	5.9	More Details
CVE-2024-30046	Visual Studio Denial of Service Vulnerability	5.9	More Details
CVE-2024-34423	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in phpbits Forty Four – 404 Plugin for WordPress allows Stored XSS.This issue affects Forty Four – 404 Plugin for WordPress: from n/a through 1.4.	5.9	More Details
CVE-2024-34425	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Phil Baylog QuickieBar allows Stored XSS.This issue affects QuickieBar: from n/a through 1.8.4.	5.9	More Details
CVE-2024-34574	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wpsoul Table Maker allows Stored XSS.This issue affects Table Maker: from n/a through 1.9.1.	5.9	More Details
CVE-2024-32985	Stellar-core is a reference implementation for the peer-to-peer agent that manages the Stellar network. Prior to 20.4.0, core nodes could be randomly crashed due to a race condition with a 3rd party library. The likelihood of affecting the network is low since crashed nodes come back up online right away. Code fix mitigation is part of Stellar-core v20.4.0 release	5.9	More Details
CVE-2024-25528	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the id parameter at /PersonalAffair/worklog_template_show.aspx.	5.9	More Details
CVE-2024-34568	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeqx LetterPress allows Stored XSS.This issue affects LetterPress: from n/a through 1.2.1.	5.9	More Details
CVE-2024-24788	A malformed DNS message in response to a query can cause the Lookup functions to get stuck in an infinite loop.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27106	Vulnerable data in transit in GE HealthCare EchoPAC products	5.7	More Details
CVE-2024-33772	A buffer overflow vulnerability in /bin/boa on D-Link DIR-619L Rev.B 2.06B1 via formTcpipSetup allows remote authenticated users to trigger a denial of service (DoS) through the parameter "curTime."	5.7	More Details
CVE-2024-32606	HDF5 Library through 1.14.3 may attempt to dereference uninitialized values in h5tools_str_sprint in tools/lib/h5tools_str.c (called from h5tools_dump_simple_data in tools/lib/h5tools_dump.c).	5.7	More Details
CVE-2024-33876	HDF5 Library through 1.14.3 has a heap buffer overflow in H5S__point_deserialize in H5Spoint.c.	5.7	More Details
CVE-2024-32607	HDF5 Library through 1.14.3 has a SEGV in H5A__close in H5Aint.c, resulting in the corruption of the instruction pointer.	5.7	More Details
CVE-2024-33875	HDF5 Library through 1.14.3 has a heap-based buffer overflow in H5O__layout_encode in H5Olayout.c, resulting in the corruption of the instruction pointer.	5.7	More Details
CVE-2024-32610	HDF5 Library through 1.14.3 has a SEGV in H5T_close_real in H5T.c, resulting in a corrupted instruction pointer.	5.7	More Details
CVE-2024-4597	An issue has been discovered in GitLab EE affecting all versions from 16.7 before 16.9.7, all versions starting from 16.10 before 16.10.5, all versions starting from 16.11 before 16.11.2. An attacker could force a user with an active SAML session to approve an MR via CSRF.	5.7	More Details
CVE-2023-50717	NocoDB is software for building databases as spreadsheets. Starting in verson 0.202.6 and prior to version 0.202.10, an attacker can upload a html file with malicious content. If user tries to open that file in browser malicious scripts can be executed leading stored cross-site scripting attack. This allows remote attacker to execute JavaScript code in the context of the user accessing the vector. An attacker could have used this vulnerability to execute requests in the name of a logged-in user or potentially collect information about the attacked user by displaying a malicious form. Version 0.202.10 contains a patch for the issue.	5.7	More Details
CVE-2024-31443	Cacti provides an operational monitoring and fault management framework. Prior to 1.2.27, some of the data stored in `form_save()` function in `data_queries.php` is not thoroughly checked and is used to concatenate the HTML statement in `grow_right_pane_tree()` function from `lib/html.php` , finally resulting in cross-site scripting. Version 1.2.27 contains a patch for the issue.	5.7	More Details
CVE-2024-4859	Solidus <= 4.3.4 is affected by a Stored Cross-Site Scripting vulnerability in the order tracking URL.	5.7	More Details
CVE-2024-29166	HDF5 through 1.14.3 contains a buffer overflow in H5O__linfo_decode, resulting in the corruption of the instruction pointer and causing denial of service or potential code execution.	5.7	More Details
CVE-2024-32993	Out-of-bounds access vulnerability in the memory module Impact: Successful exploitation of this vulnerability will affect availability.	5.6	More Details
CVE-2024-30801	SQL Injection vulnerability in Cloud based customer service management platform v.1.0.0 allows a local attacker to execute arbitrary code via a crafted payload to Login.asp component.	5.5	More Details
CVE-2024-0098	NVIDIA ChatRTX for Windows contains a vulnerability in the ChatRTX UI and backend, where a user can cause a clear-text transmission of sensitive information issue by data sniffing. A successful exploit of this vulnerability might lead to information disclosure.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27393	In the Linux kernel, the following vulnerability has been resolved: xen-netfront: Add missing skb_mark_for_recycle Notice that skb_mark_for_recycle() is introduced later than fixes tag in commit 6a5bcd84e886 ("page_pool: Allow drivers to hint on SKB recycling"). It is believed that fixes tag were missing a call to page_pool_release_page() between v5.9 to v5.14, after which is should have used skb_mark_for_recycle(). Since v6.6 the call page_pool_release_page() were removed (in commit 535b9c61bdef ("net: page_pool: hide page_pool_release_page()") and remaining callers converted (in commit 6bfef2ec0172 ("Merge branch 'net-page_pool-remove-page_pool_release_page'")). This leak became visible in v6.8 via commit dba1b8a7ab68 ("mm/page_pool: catch page_pool memory leaks").	5.5	More Details
CVE-2024-30008	Windows DWM Core Library Information Disclosure Vulnerability	5.5	More Details
CVE-2024-27827	This issue was addressed through improved state management. This issue is fixed in macOS Sonoma 14.5. An app may be able to read arbitrary files.	5.5	More Details
CVE-2024-30039	Windows Remote Access Connection Manager Information Disclosure Vulnerability	5.5	More Details
CVE-2024-4693	A flaw was found in the QEMU Virtio PCI Bindings (hw/virtio/virtio-pci.c). An improper release and use of the irqfd for vector 0 during the boot process leads to a guest triggerable crash via vhost_net_stop(). This flaw allows a malicious guest to crash the QEMU process on the host.	5.5	More Details
CVE-2024-34353	The matrix-sdk-crypto crate, part of the Matrix Rust SDK project, is an implementation of a Matrix end-to-end encryption state machine in Rust. In Matrix, the server-side `key backup` stores encrypted copies of Matrix message keys. This facilitates key sharing between a user's devices and provides a redundant copy in case all devices are lost. The key backup uses asymmetric cryptography, with each server-side key backup assigned a unique public-private key pair. Due to a logic bug introduced in commit 71136e44c03c79f80d6d1a2446673bc4d53a2067, matrix-sdk-crypto version 0.7.0 will sometimes log the private part of the backup key pair to Rust debug logs (using the `tracing` crate). This issue has been resolved in matrix-sdk-crypto version 0.7.1. No known workarounds are available.	5.5	More Details
CVE-2024-23229	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Monterey 12.7.5, macOS Ventura 13.6.5, macOS Sonoma 14.4. A malicious application may be able to access Find My data.	5.5	More Details
CVE-2024-23236	A correctness issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.5. An app may be able to read arbitrary files.	5.5	More Details
CVE-2024-30016	Windows Cryptographic Services Information Disclosure Vulnerability	5.5	More Details
CVE-2024-27816	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.5 and iPadOS 17.5, tvOS 17.5, watchOS 10.5, macOS Sonoma 14.5. An attacker may be able to access user data.	5.5	More Details
CVE-2024-33866	An issue was discovered in linqi before 1.4.0.1 on Windows. There is /api/DocumentTemplate/{GUID] XSS.	5.5	More Details
CVE-2024-0088	NVIDIA Triton Inference Server for Linux contains a vulnerability in shared memory APIs, where a user can cause an improper memory access issue by a network API. A successful exploit of this vulnerability might lead to denial of service and data tampering.	5.5	More Details
CVE-2024-30037	Windows Common Log File System Driver Elevation of Privilege Vulnerability	5.5	More Details
CVE-2024-27834	The issue was addressed with improved checks. This issue is fixed in iOS 17.5 and iPadOS 17.5, tvOS 17.5, Safari 17.5, watchOS 10.5, macOS Sonoma 14.5. An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27841	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.5 and iPadOS 17.5, macOS Sonoma 14.5. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2023-5447	Missing lock check in SynHsaService may create a use-after-free condition which causes abnormal termination of the service, resulting in denial of service for the Synaptics Hardware Support App.	5.5	More Details
CVE-2024-27847	This issue was addressed with improved checks This issue is fixed in iOS 17.5 and iPadOS 17.5, macOS Sonoma 14.5. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2023-50180	An exposure of sensitive system information to an unauthorized control sphere vulnerability [CWE-497] in FortiADC version 7.4.1 and below, version 7.2.3 and below, version 7.1.4 and below, version 7.0.5 and below, version 6.2.6 and below may allow a read-only admin to view data pertaining to other admins.	5.5	More Details
CVE-2024-32731	SAP My Travel Requests does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. On successful exploitation, the attacker can upload a malicious attachment to a business trip request which will lead to a low impact on the confidentiality, integrity and availability of the application.	5.5	More Details
CVE-2024-30034	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2024-4840	An flaw was found in the OpenStack Platform (RHOSP) director, a toolset for installing and managing a complete RHOSP environment. Plaintext passwords may be stored in log files, which can expose sensitive information to anyone with access to the logs.	5.5	More Details
CVE-2024-27789	A logic issue was addressed with improved checks. This issue is fixed in iOS 16.7.8 and iPadOS 16.7.8, macOS Monterey 12.7.5, macOS Ventura 13.6.7, macOS Sonoma 14.4. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-27810	A path handling issue was addressed with improved validation. This issue is fixed in iOS 17.5 and iPadOS 17.5, tvOS 17.5, watchOS 10.5, macOS Sonoma 14.5. An app may be able to read sensitive location information.	5.5	More Details
CVE-2024-27804	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.5 and iPadOS 17.5, tvOS 17.5, watchOS 10.5, macOS Sonoma 14.5. An app may be able to execute arbitrary code with kernel privileges.	5.5	More Details
CVE-2024-4562	In WhatsUp Gold versions released before 2023.1.2 , an SSRF vulnerability exists in Whatsup Gold's Issue exists in the HTTP Monitoring functionality. Due to the lack of proper authorization, any authenticated user can access the HTTP monitoring functionality, what leads to the Server Side Request Forgery.	5.4	More Details
CVE-2024-3241	The Ultimate Blocks WordPress plugin before 3.1.7 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2024-34357	TYPO3 is an enterprise content management system. Starting in version 9.0.0 and prior to versions 9.5.48 ELTS, 10.4.45 ELTS, 11.5.37 LTS, 12.4.15 LTS, and 13.1.1, failing to properly encode user-controlled values in file entities, the `ShowImageController` (`_eID tx_cms_showpic_`) is vulnerable to cross-site scripting. Exploiting this vulnerability requires a valid backend user account with access to file entities. TYPO3 versions 9.5.48 ELTS, 10.4.45 ELTS, 11.5.37 LTS, 12.4.15 LTS, 13.1.1 fix the problem described.	5.4	More Details
CVE-2024-30041	Microsoft Bing Search Spoofing Vulnerability	5.4	More Details
CVE-2024-35011	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/infoType_deal.php?mudi=rev&nohrefStr=close.	5.4	More Details
CVE-2024-30050	Windows Mark of the Web Security Feature Bypass Vulnerability	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4860	The 'WordPress RSS Aggregator' WordPress Plugin, versions < 4.23.9 are affected by a Cross-Site Scripting (XSS) vulnerability due to the lack of sanitization of the 'notice_id' GET parameter.	5.4	More Details
CVE-2023-24203	Cross Site Scripting vulnerability in SourceCodester Simple Customer Relationship Management System v1.0 allows attacker to execute arbitary code via the company or query parameter(s).	5.4	More Details
CVE-2023-24204	SQL injection vulnerability in SourceCodester Simple Customer Relationship Management System v1.0 allows attacker to execute arbitrary code via the name parameter in get-quote.php.	5.4	More Details
CVE-2024-32077	Apache Airflow version 2.9.0 has a vulnerability that allows an authenticated attacker to inject malicious data into the task instance logs. Users are recommended to upgrade to version 2.9.1, which fixes this issue.	5.4	More Details
CVE-2024-34356	TYPO3 is an enterprise content management system. Starting in version 9.0.0 and prior to versions 9.5.48 ELTS, 10.4.45 ELTS, 11.5.37 LTS, 12.4.15 LTS, and 13.1.1, the form manager backend module is vulnerable to cross-site scripting. Exploiting this vulnerability requires a valid backend user account with access to the form module. TYPO3 versions 9.5.48 ELTS, 10.4.45 ELTS, 11.5.37 LTS, 12.4.15 LTS, and 13.1.1 fix the problem described.	5.4	More Details
CVE-2024-3462	Ant Media Server Community Edition in a default configuration is vulnerable to an improper HTTP header based authorization, leading to a possible use of non-administrative API calls reserved only for authorized users. All versions up to 2.9.0 (tested) and possibly newer ones are believed to be vulnerable as the vendor has not confirmed releasing a patch.	5.4	More Details
CVE-2024-4606	Deserialization of Untrusted Data vulnerability in BdThemes Ultimate Store Kit Elementor Addons.This issue affects Ultimate Store Kit Elementor Addons: from n/a through 2.0.3.	5.4	More Details
CVE-2024-4425	The access control in CemiPark software stores integration (e.g. FTP or SIP) credentials in plain-text. An attacker who gained unauthorized access to the device can retrieve clear text passwords used by the system.This issue affects CemiPark software: 4.5, 4.7, 5.03 and potentially others. The vendor refused to provide the specific range of affected products.	5.4	More Details
CVE-2024-30055	Microsoft Edge (Chromium-based) Spoofing Vulnerability	5.4	More Details
CVE-2024-34709	Directus is a real-time API and App dashboard for managing SQL database content. Prior to 10.11.0, session tokens function like the other JWT tokens where they are not actually invalidated when logging out. The `directus_session` gets destroyed and the cookie gets deleted but if the cookie value is captured, it will still work for the entire expiry time which is set to 1 day by default. Making it effectively a long lived unrevokable stateless token instead of the stateful session token it was meant to be. This vulnerability is fixed in 10.11.0.	5.4	More Details
CVE-2024-3956	The Pods – Custom Content Types and Fields plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Pod Form widget in all versions up to, and including, 3.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2024-32674	Heateor Social Login WordPress prior to 1.1.32 contains a cross-site scripting vulnerability. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the user who accessed the website using the product.	5.4	More Details
CVE-2024-34814	Cross-Site Request Forgery (CSRF) vulnerability in ThemeFuse Unyson.This issue affects Unyson: from n/a through 2.7.29.	5.4	More Details
CVE-2024-34816	Cross-Site Request Forgery (CSRF) vulnerability in Revmakx WPCal.Io – Easy Meeting Scheduler.This issue affects WPCal.Io – Easy Meeting Scheduler: from n/a through 0.9.5.8.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4135	The WP Latest Posts plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 5.0.7. This is due to the plugin allowing users to execute an action that does not properly validate a user-supplied value prior to using that value in a call to do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	5.4	More Details
CVE-2024-28761	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.25 and 12.0.1.0 through 12.0.12.0 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 285245.	5.4	More Details
CVE-2024-3239	The Post Grid Gutenberg Blocks and WordPress Blog Plugin WordPress plugin before 4.0.2 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2024-29894	Cacti provides an operational monitoring and fault management framework. Versions of Cacti prior to 1.2.27 contain a residual cross-site scripting vulnerability caused by an incomplete fix for CVE-2023-50250. `raise_message_javascript` from `lib/functions.php` now uses purify.js to fix CVE-2023-50250 (among others). However, it still generates the code out of unescaped PHP variables `$title` and `$header`. If those variables contain single quotes, they can be used to inject JavaScript code. An attacker exploiting this vulnerability could execute actions on behalf of other users. This ability to impersonate users could lead to unauthorized changes to settings. Version 1.2.27 fixes this issue.	5.4	More Details
CVE-2024-3722	The Swift Performance Lite plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the ajax_handler() function in all versions up to, and including, 2.3.6.18. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve and modify settings.	5.4	More Details
CVE-2024-28781	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.20, 7.1 through 7.1.2.16, 7.2 through 7.2.3.9, 7.3 through 7.3.2.4, and 8.0 through 8.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 285654.	5.4	More Details
CVE-2024-32100	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Easy Digital Downloads.This issue affects Easy Digital Downloads: from n/a through 3.2.11.	5.3	More Details
CVE-2024-35166	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ninja Team Filebird.This issue affects Filebird: from n/a through 5.6.3.	5.3	More Details
CVE-2024-4280	The White Label CMS plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the reset_plugin function in all versions up to, and including, 2.7.3. This makes it possible for unauthenticated attackers to reset plugin settings.	5.3	More Details
CVE-2024-35165	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Gutenify.This issue affects Gutenify: from n/a through 1.4.0.	5.3	More Details
CVE-2024-32719	Missing Authorization vulnerability in WP Club Manager.This issue affects WP Club Manager: from n/a through 2.2.11.	5.3	More Details
CVE-2024-31486	A vulnerability has been identified in OPUPI0 AMQP/MQTT (All versions < V5.30). The affected devices stores MQTT client passwords without sufficient protection on the devices. An attacker with remote shell access or physical access could retrieve the credentials leading to confidentiality loss.	5.3	More Details
CVE-2024-3374	An unauthenticated user can trigger a fatal assertion in the server while generating ftdc diagnostic metrics due to attempting to build a BSON object that exceeds certain memory sizes. This issue affects MongoDB Server v5.0 versions prior to and including 5.0.16 and MongoDB Server v6.0 versions prior to and including 6.0.5.	5.3	More Details
CVE-2024-26007	An improper check or handling of exceptional conditions vulnerability [CWE-703] in Fortinet FortiOS version 7.4.1 allows an unauthenticated attacker to provoke a denial of service on the administrative interface via crafted HTTP requests.	5.3	More Details
CVE-2024-32669	Improper Input Validation vulnerability in Samsung Open Source escargot JavaScript engine allows Overflow Buffers. However, it occurs in the test code and does not include in the release. This issue affects escargot: 4.0.0.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6327	The ShopLentor (formerly WooLentor) plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the purchased_new_products function in all versions up to, and including, 2.8.7. This makes it possible for unauthenticated attackers to view all products purchased in the past week, along with the users that purchased them.	5.3	More Details
CVE-2024-1229	The SimpleShop plugin for WordPress is vulnerable to unauthorized disconnection from SimpleShop due to a missing capability check on the maybe_disconnect_simpleshop function in all versions up to, and including, 2.10.2. This makes it possible for unauthenticated attackers to disconnect the SimpleShop.	5.3	More Details
CVE-2024-34812	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in RadiusTheme ShopBuilder – Elementor WooCommerce Builder Addons.This issue affects ShopBuilder – Elementor WooCommerce Builder Addons: from n/a through 2.1.8.	5.3	More Details
CVE-2024-35171	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Academy LMS academy.This issue affects Academy LMS: from n/a through 1.9.25.	5.3	More Details
CVE-2024-4444	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to bypass to user registration in versions up to, and including, 4.2.6.5. This is due to missing checks in the 'create_account' function in the checkout. This makes it possible for unauthenticated attackers to register as the default role on the site, even if registration is disabled.	5.3	More Details
CVE-2024-32672	A Segmentation Fault issue discovered in Samsung Open Source Escargot JavaScript engine allows remote attackers to cause a denial of service via crafted input. This issue affects Escargot: 4.0.0.	5.3	More Details
CVE-2024-4213	The Shopping Cart & eCommerce Store plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 5.6.4 via the order report functionality. This makes it possible for unauthenticated attackers to extract sensitive data including order details such as payment details, addresses and other PII.	5.3	More Details
CVE-2024-34717	PrestaShop is an open source e-commerce web application. In PrestaShop 8.1.5, any invoice can be downloaded from front-office in anonymous mode, by supplying a random secure_key parameter in the url. This issue is patched in version 8.1.6. No known workarounds are available.	5.3	More Details
CVE-2024-25966	Dell PowerScale OneFS versions 8.2.x through 9.7.0.2 contains an improper handling of unexpected data type vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service.	5.3	More Details
CVE-2024-35175	sshpiper is a reverse proxy for sshd. Starting in version 1.0.50 and prior to version 1.3.0, the way the proxy protocol listener is implemented in sshpiper can allow an attacker to forge their connecting address. Commit 2ddd69876a1e1119059debc59fe869cb4e754430 added the proxy protocol listener as the only listener in sshpiper, with no option to toggle this functionality off. This means that any connection that sshpiper is directly (or in some cases indirectly) exposed to can use proxy protocol to forge its source address. Any users of sshpiper who need logs from it for whitelisting/rate limiting/security investigations could have them become much less useful if an attacker is sending a spoofed source address. Version 1.3.0 contains a patch for the issue.	5.3	More Details
CVE-2024-4818	A vulnerability was found in Campcodes Online Laundry Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /index.php. 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 associated identifier of this vulnerability is VDB-263939.	5.3	More Details
CVE-2024-31482	An unauthenticated Denial-of-Service (DoS) vulnerability exists in the ANSI escape code service accessed via the PAPI protocol. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected Access Point.	5.3	More Details
CVE-2024-31481	Unauthenticated Denial of Service (DoS) vulnerabilities exist in the CLI service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to interrupt the normal operation of the affected service.	5.3	More Details
CVE-2024-31480	Unauthenticated Denial of Service (DoS) vulnerabilities exist in the CLI service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to interrupt the normal operation of the affected service.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31479	Unauthenticated Denial of Service (DoS) vulnerabilities exist in the Central Communications service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to interrupt the normal operation of the affected service.	5.3	More Details
CVE-2024-31478	Multiple unauthenticated Denial-of-Service (DoS) vulnerabilities exists in the Soft AP daemon accessed via the PAPI protocol. Successful exploitation of these vulnerabilites result in the ability to interrupt the normal operation of the affected Access Point.	5.3	More Details
CVE-2024-34914	php-censor v2.1.4 and fixed in v.2.1.5 was discovered to utilize a weak hashing algorithm for its remember_key value. This allows attackers to bruteforce to bruteforce the remember_key value to gain access to accounts that have checked "remember me" when logging in.	5.3	More Details
CVE-2024-33498	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected applications do not properly release memory that is allocated when handling specifically crafted incoming packets. This could allow an unauthenticated remote attacker to cause a denial of service condition by crashing the service when it runs out of memory. The service is restarted automatically after a short time.	5.3	More Details
CVE-2024-34080	MantisBT (Mantis Bug Tracker) is an open source issue tracker. If an issue references a note that belongs to another issue that the user doesn't have access to, then it gets hyperlinked. Clicking on the link gives an access denied error as expected, yet some information remains available via the link, link label, and tooltip. This can result in disclosure of the existence of the note, the note author name, the note creation timestamp, and the issue id the note belongs to. Version 2.26.2 contains a patch for the issue. No known workarounds are available.	5.3	More Details
CVE-2024-0870	The YITH WooCommerce Gift Cards plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'save_mail_status' and 'save_email_settings' functions in all versions up to, and including, 4.12.0. This makes it possible for unauthenticated attackers to modify WooCommerce settings.	5.3	More Details
CVE-2024-3915	The Swift Framework plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the sf_edit_directory_item() function in all versions up to, and including, 2.7.31. This makes it possible for unauthenticated attackers to update arbitrary posts with arbitrary content. Unfortunately, we did not receive a response from the vendor to send over the vulnerability details.	5.3	More Details
CVE-2024-30459	Missing Authorization vulnerability in AIpost AI WP Writer.This issue affects AI WP Writer: from n/a through 3.6.5.	5.3	More Details
CVE-2024-3916	The Swift Framework plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of the plugin's shortcodes in all versions up to, and including, 2.7.31 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Unfortunately, we did not receive a response from the vendor to send over the vulnerability details.	5.3	More Details
CVE-2024-34549	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Automattic WP Job Manager.This issue affects WP Job Manager: from n/a through 2.2.2.	5.3	More Details
CVE-2024-34550	Insertion of Sensitive Information into Log File vulnerability in AlexaCRM Dynamics 365 Integration.This issue affects Dynamics 365 Integration: from n/a through 1.3.17.	5.3	More Details
CVE-2024-34556	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in UkrSolution Barcode Scanner with Inventory & Order Manager.This issue affects Barcode Scanner with Inventory & Order Manager: from n/a through 1.5.4.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4067	The NPM package `micromatch` prior to 4.0.8 is vulnerable to Regular Expression Denial of Service (ReDoS). The vulnerability occurs in `micromatch.braces()` in `index.js` because the pattern `.*` will greedily match anything. By passing a malicious payload, the pattern matching will keep backtracking to the input while it doesn't find the closing bracket. As the input size increases, the consumption time will also increase until it causes the application to hang or slow down. There was a merged fix but further testing shows the issue persists. This issue should be mitigated by using a safe pattern that won't start backtracking the regular expression due to greedy matching. This issue was fixed in version 4.0.8.	5.3	More Details
CVE-2024-27947	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.5). The affected systems could allow log messages to be forwarded to a specific client under certain circumstances. An attacker could leverage this vulnerability to forward log messages to a specific compromised client.	5.3	More Details
CVE-2024-34358	TYPO3 is an enterprise content management system. Starting in version 9.0.0 and prior to versions 9.5.48 ELTS, 10.4.45 ELTS, 11.5.37 LTS, 12.4.15 LTS, and 13.1.1, the `ShowImageController` (`_eID tx_cms_showpic_`) lacks a cryptographic HMAC-signature on the `frame` HTTP query parameter (e.g. `/index.php?eID=tx_cms_showpic?file=3&...&frame=12345`). This allows adversaries to instruct the system to produce an arbitrary number of thumbnail images on the server side. TYPO3 versions 9.5.48 ELTS, 10.4.45 ELTS, 11.5.37 LTS, 12.4.15 LTS, 13.1.1 fix the problem described.	5.3	More Details
CVE-2024-28135	A low privileged remote attacker can use a command injection vulnerability in the API which performs remote code execution as the user-app user due to improper input validation. The confidentiality is partly affected.	5.0	More Details
CVE-2023-45586	An insufficient verification of data authenticity vulnerability [CWE-345] in Fortinet FortiOS SSL-VPN tunnel mode version 7.4.0 through 7.4.1, version 7.2.0 through 7.2.7 and before 7.0.12 & FortiProxy SSL-VPN tunnel mode version 7.4.0 through 7.4.1, version 7.2.0 through 7.2.7 and before 7.0.13 allows an authenticated VPN user to send (but not receive) packets spoofing the IP of another user via crafted network packets.	5.0	More Details
CVE-2024-0862	The Proofpoint Encryption endpoint of Proofpoint Enterprise Protection contains a Server-Side Request Forgery vulnerability that allows an authenticated user to relay HTTP requests from the Protection server to otherwise private network addresses.	5.0	More Details
CVE-2024-33008	SAP Replication Server allows an attacker to use gateway for executing some commands to RSSD. This could result in crashing the Replication Server due to memory corruption with high impact on Availability of the system.	4.9	More Details
CVE-2024-32886	Vitess is a database clustering system for horizontal scaling of MySQL. When executing the following simple query, the `vtgate` will go into an endless loop that also keeps consuming memory and eventually will run out of memory. This vulnerability is fixed in 19.0.4, 18.0.5, and 17.0.7.	4.9	More Details
CVE-2024-31483	An authenticated sensitive information disclosure vulnerability exists in the CLI service accessed via the PAPI protocol. Successful exploitation of this vulnerability results in the ability to read arbitrary files in the underlying operating system.	4.9	More Details
CVE-2024-34708	Directus is a real-time API and App dashboard for managing SQL database content. A user with permission to view any collection using redacted hashed fields can get access the raw stored version using the `alias` functionality on the API. Normally, these redacted fields will return `**********` however if we change the request to `?alias[workaround]=redacted` we can instead retrieve the plain text value for the field. This can be avoided by removing permission to view the sensitive fields entirely from users or roles that should not be able to see them. This vulnerability is fixed in 10.11.0.	4.9	More Details
CVE-2023-42955	Claris International has successfully resolved an issue of potentially exposing password information to front-end websites when signed in to the Admin Console with an administrator role. This issue has been fixed in FileMaker Server 20.3.1 by eliminating the send of Admin Role passwords in the Node.js socket.	4.9	More Details
CVE-2024-3794	Vulnerability in WBSAirback 21.02.04, which consists of a stored Cross-Site Scripting (XSS) through /admin/AdvancedSystem, description field, all parameters. Exploitation of this vulnerability could allow a remote user to send a specially crafted URL to the victim and steal their session data.	4.8	More Details
CVE-2024-3793	Vulnerability in WBSAirback 21.02.04, which consists of a stored Cross-Site Scripting (XSS) through /admin/CloudAccounts, account name / user password / server fields, all parameters. Exploitation of this vulnerability could allow a remote user to send a specially crafted URL to the victim and steal their session data.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33867	An issue was discovered in linqi before 1.4.0.1 on Windows. There is a hardcoded password salt.	4.8	More Details
CVE-2024-3796	Vulnerability in WBSAirback 21.02.04, which consists of a stored Cross-Site Scripting (XSS) through /admin/BackupSchedule, description field. Exploitation of this vulnerability could allow a remote user to send a specially crafted URL to the victim and steal their session data.	4.8	More Details
CVE-2024-3795	Vulnerability in WBSAirback 21.02.04, which consists of a stored Cross-Site Scripting (XSS) through /admin/BackupTemplate, name / description fields. Exploitation of this vulnerability could allow a remote user to send a specially crafted URL to the victim and steal their session data.	4.8	More Details
CVE-2023-5971	The Save as PDF Plugin by Pdfcrowd WordPress plugin before 3.2.0 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-2024-33433	Cross Site Scripting vulnerability in TOTOLINK X2000R before v1.0.0-B20231213.1013 allows a remote attacker to execute arbitrary code via the Guest Access Control parameter in the Wireless Page.	4.8	More Details
CVE-2024-34349	Sylius is an open source eCommerce platform. Prior to 1.12.16 and 1.13.1, there is a possibility to execute javascript code in the Admin panel. In order to perform an XSS attack input a script into Name field in which of the resources: Taxons, Products, Product Options or Product Variants. The code will be executed while using an autocomplete field with one of the listed entities in the Admin Panel. Also for the taxons in the category tree on the product form.The issue is fixed in versions: 1.12.16, 1.13.1.	4.8	More Details
CVE-2024-3791	Vulnerability in WBSAirback 21.02.04, which consists of a stored Cross-Site Scripting (XSS) through /admin/SystemConfiguration, name / free memory limit fields , type / password parameters. Exploitation of this vulnerability could allow a remote user to send a specially crafted URL to the victim and steal their session data.	4.8	More Details
CVE-2024-3792	Vulnerability in WBSAirback 21.02.04, which consists of a stored Cross-Site Scripting (XSS) through /admin/DeviceReplication, execution range field, all parameters. Exploitation of this vulnerability could allow a remote user to send a specially crafted URL to the victim and steal their session data.	4.8	More Details
CVE-2024-3790	Vulnerability in WBSAirback 21.02.04, which consists of a stored Cross-Site Scripting (XSS) through /admin/SystemUsers, login / description fields, passwd1/ passwd2 parameters. Exploitation of this vulnerability could allow a remote user to send a specially crafted URL to the victim and steal their session data.	4.8	More Details
CVE-2023-52384	Double-free vulnerability in the RSMC module Impact: Successful exploitation of this vulnerability will affect availability.	4.7	More Details
CVE-2023-52383	Double-free vulnerability in the RSMC module Impact: Successful exploitation of this vulnerability will affect availability.	4.7	More Details
CVE-2024-27202	A DOM-based cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.7	More Details
CVE-2024-27821	A path handling issue was addressed with improved validation. This issue is fixed in iOS 17.5 and iPadOS 17.5, watchOS 10.5, macOS Sonoma 14.5. A shortcut may output sensitive user data without consent.	4.7	More Details
CVE-2024-4681	A vulnerability, which was classified as critical, was found in Campcodes Legal Case Management System 1.0. Affected is an unknown function of the file /admin/general-setting of the component Setting Handler. The manipulation of the argument favicon/logo leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-263622 is the identifier assigned to this vulnerability.	4.7	More Details
CVE-2024-31444	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, some of the data stored in `automation_tree_rules_form_save()` function in `automation_tree_rules.php` is not thoroughly checked and is used to concatenate the HTML statement in `form_confirm()` function from `lib/html.php` , finally resulting in cross-site scripting. Version 1.2.27 contains a patch for the issue.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31458	Cacti provides an operational monitoring and fault management framework. Prior to version 1.2.27, some of the data stored in `form_save()` function in `graph_template_inputs.php` is not thoroughly checked and is used to concatenate the SQL statement in `draw_nontemplated_fields_graph_item()` function from `lib/html_form_templates.php` , finally resulting in SQL injection. Version 1.2.27 contains a patch for the issue.	4.6	More Details
CVE-2024-4231	This vulnerability exists in Digisol Router (DG-GR1321: Hardware version 3.7L; Firmware version : v3.2.02) due to presence of root terminal access on a serial interface without proper access control. An attacker with physical access could exploit this by identifying UART pins and accessing the root shell on the vulnerable system. Successful exploitation of this vulnerability could allow the attacker to access the sensitive information on the targeted system.	4.6	More Details
CVE-2024-34698	FreeScout is a free, self-hosted help desk and shared mailbox. Versions of FreeScout prior to 1.8.139 contain a Prototype Pollution vulnerability in the `/public/js/main.js` source file. The Prototype Pollution arises because the `getQueryParam` Function recursively merges an object containing user-controllable properties into an existing object (For URL Query Parameters Parsing), without first sanitizing the keys. This can allow an attacker to inject a property with a key `__proto__`, along with arbitrarily nested properties. The merge operation assigns the nested properties to the `params` object's prototype instead of the target object itself. As a result, the attacker can pollute the prototype with properties containing harmful values, which are then inherited by user-defined objects and subsequently used by the application dangerously. The vulnerability lets an attacker control properties of objects that would otherwise be inaccessible. If the application subsequently handles an attacker-controlled property in an unsafe way, this can potentially be chained with other vulnerabilities like DOM-based XSS, Open Redirection, Cookie Manipulation, Link Manipulation, HTML Injection, etc. Version 1.8.139 contains a patch for the issue.	4.6	More Details
CVE-2024-33819	Globitel KSA SpeechLog v8.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Save Query function.	4.6	More Details
CVE-2024-27281	An issue was discovered in RDoc 6.3.3 through 6.6.2, as distributed in Ruby 3.x through 3.3.0. When parsing .rdoc_options (used for configuration in RDoc) as a YAML file, object injection and resultant remote code execution are possible because there are no restrictions on the classes that can be restored. (When loading the documentation cache, object injection and resultant remote code execution are also possible if there were a crafted cache.) The main fixed version is 6.6.3.1. For Ruby 3.0 users, a fixed version is rdoc 6.3.4.1. For Ruby 3.1 users, a fixed version is rdoc 6.4.1.1. For Ruby 3.2 users, a fixed version is rdoc 6.5.1.1.	4.5	More Details
CVE-2024-34433	Deserialization of Untrusted Data vulnerability in OCDI One Click Demo Import.This issue affects One Click Demo Import: from n/a through 3.2.0.	4.4	More Details
CVE-2024-4162	A buffer error in Panasonic KW Watcher versions 1.00 through 2.83 may allow attackers malicious read access to memory.	4.4	More Details
CVE-2024-2846	The Visual Footer Credit Remover plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'selector' parameter in all versions up to, and including, 2 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. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-28132	Exposure of Sensitive Information vulnerability exists in the GSLB container, which may allow an authenticated attacker with local access to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.4	More Details
CVE-2024-3068	The Custom Field Suite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cfs[fields][*][name]' parameter in all versions up to, and including, 2.6.5 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. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-35172	Server-Side Request Forgery (SSRF) vulnerability in ShortPixel ShortPixel Adaptive Images.This issue affects ShortPixel Adaptive Images: from n/a through 3.8.3.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4417	The Falang multilanguage for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.3.49 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-2024-34439	Cross-Site Request Forgery (CSRF) vulnerability in divSpot DS Site Message.This issue affects DS Site Message: from n/a through 1.14.4.	4.3	More Details
CVE-2024-34557	Cross-Site Request Forgery (CSRF) vulnerability in UkrSolution Barcode Scanner with Inventory & Order Manager.This issue affects Barcode Scanner with Inventory & Order Manager: from n/a through 1.5.4.	4.3	More Details
CVE-2024-34827	Cross-Site Request Forgery (CSRF) vulnerability in Cozmoslabs, Razvan Mocanu, Madalin Ungureanu, Cristophor Hurduban TranslatePress.This issue affects TranslatePress: from n/a through 2.7.5.	4.3	More Details
CVE-2024-35048	An issue in SurveyKing v1.3.1 allows attackers to execute a session replay attack after a user changes their password.	4.3	More Details
CVE-2024-34427	Cross-Site Request Forgery (CSRF) vulnerability in Huseyin Berberoglu WP Favorite Posts.This issue affects WP Favorite Posts: from n/a through 1.6.8.	4.3	More Details
CVE-2023-6812	The WP Compress – Image Optimizer [All-In-One plugin for WordPress is vulnerable to Open Redirect in all versions up to, and including, 6.20.01. This is due to insufficient validation on the redirect url supplied via the 'css' parameter. This makes it possible for unauthenticated attackers to redirect users to potentially malicious sites if they can successfully trick them into performing an action.	4.3	More Details
CVE-2024-34828	Cross-Site Request Forgery (CSRF) vulnerability in Andy Moyle Church Admin.This issue affects Church Admin: from n/a through 4.1.32.	4.3	More Details
CVE-2024-34817	Cross-Site Request Forgery (CSRF) vulnerability in CRM Perks Integration for Pipedrive and Contact Form 7, WPForms, Elementor, Ninja Forms.This issue affects Integration for Pipedrive and Contact Form 7, WPForms, Elementor, Ninja Forms: from n/a through 1.2.0.	4.3	More Details
CVE-2024-34823	Cross-Site Request Forgery (CSRF) vulnerability in Kiboko Labs Arigato Autoresponder and Newsletter.This issue affects Arigato Autoresponder and Newsletter: from n/a through 2.7.2.3.	4.3	More Details
CVE-2024-4138	Manage Bank Statement ReProcessing Rules does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. By exploiting this vulnerability, an attacker can enable/disable the sharing rule of other users affecting the integrity of the application. Confidentiality and Availability are not affected.	4.3	More Details
CVE-2024-4139	Manage Bank Statement ReProcessing Rules does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. By exploiting this vulnerability, an attacker can delete rules of other users affecting the integrity of the application. Confidentiality and Availability are not affected.	4.3	More Details
CVE-2024-34825	Cross-Site Request Forgery (CSRF) vulnerability in Warfare Plugins Social Warfare.This issue affects Social Warfare: from n/a through 4.4.5.1.	4.3	More Details
CVE-2024-34223	Insecure permission vulnerability in /hrm/leaverequest.php in SourceCodester Human Resource Management System 1.0 allow attackers to approve or reject leave ticket.	4.3	More Details
CVE-2024-1693	The SP Project & Document Manager plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the cdm_save_category AJAX action in all versions up to, and including, 4.70. This makes it possible for authenticated attackers, with subscriber-level access and above, to update arbitrary folder name that do not belong to them.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4233	Missing Authorization vulnerability in Tyche Softwares Print Invoice & Delivery Notes for WooCommerce, Tyche Softwares Arconix Shortcodes, Tyche Softwares Arconix FAQ.This issue affects Print Invoice & Delivery Notes for WooCommerce: from n/a through 4.8.1; Arconix Shortcodes: from n/a through 2.1.10; Arconix FAQ: from n/a through 1.9.3.	4.3	More Details
CVE-2024-4766	Different techniques existed to obscure the fullscreen notification in Firefox for Android. These could have led to potential user confusion and spoofing attacks. *This bug only affects Firefox for Android. Other versions of Firefox are unaffected.* This vulnerability affects Firefox < 126.	4.3	More Details
CVE-2024-4689	Cross-Site Request Forgery (CSRF) vulnerability in ShortPixel ShortPixel Adaptive Images.This issue affects ShortPixel Adaptive Images: from n/a through 3.8.3.	4.3	More Details
CVE-2024-33574	Missing Authorization vulnerability in appsbd Vitepos.This issue affects Vitepos: from n/a through 3.0.1.	4.3	More Details
CVE-2024-33573	Missing Authorization vulnerability in EPROLO EPROLO Dropshipping.This issue affects EPROLO Dropshipping: from n/a through 1.7.1.	4.3	More Details
CVE-2024-1230	The SimpleShop plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.10.0. This is due to missing or incorrect nonce validation on the maybe_disconnect_simpleshop function. This makes it possible for unauthenticated attackers to disconnect the site from simpleshop 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-2024-1467	The Starter Templates — Elementor, WordPress & Beaver Builder Templates plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.1.6 via the ai_api_request(). This makes it possible for authenticated attackers, with contributor-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	4.3	More Details
CVE-2024-33956	Missing Authorization vulnerability in ThemeLocation Custom WooCommerce Checkout Fields Editor.This issue affects Custom WooCommerce Checkout Fields Editor: from n/a through 1.3.0.	4.3	More Details
CVE-2024-24833	Missing Authorization vulnerability in Leevio Happy Addons for Elementor.This issue affects Happy Addons for Elementor: from n/a through 3.10.1.	4.3	More Details
CVE-2024-28759	A crafted network packet may cause a buffer overrun in Wind River VxWorks 7 through 23.09.	4.3	More Details
CVE-2024-28760	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.25 and 12.0.1.0 through 12.0.12.0 dashboard is vulnerable to a denial of service due to improper restrictions of resource allocation. IBM X-Force ID: 285244.	4.3	More Details
CVE-2024-31113	Cross-Site Request Forgery (CSRF) vulnerability in Easy Digital Downloads.This issue affects Easy Digital Downloads: from n/a through 3.2.11.	4.3	More Details
CVE-2024-4539	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 prior to 16.9.7, starting from 16.10 prior to 16.10.5, and starting from 16.11 prior to 16.11.2 where abusing the API to filter branch and tags could lead to Denial of Service.	4.3	More Details
CVE-2024-4463	The Squelch Tabs and Accordions Shortcodes plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.4.7. This is due to missing or incorrect nonce validation when saving plugin settings. This makes it possible for unauthenticated attackers to modify plugin settings 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-2024-33004	SAP Business Objects Business Intelligence Platform is vulnerable to Insecure Storage as dynamic web pages are getting cached even after logging out. On successful exploitation, the attacker can see the sensitive information through cache and can open the pages causing limited impact on Confidentiality, Integrity and Availability of the application.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4314	The Hostel plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.5.3. This is due to missing or incorrect nonce validation when managing rooms. This makes it possible for unauthenticated attackers to create and delete rooms 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-2024-4312	The Soccer Engine – Soccer Plugin for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.12. This is due to missing or incorrect nonce validation when saving match and team settings. This makes it possible for unauthenticated attackers to change plugin settings as well as teams, players, etc. 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-2024-4790	A vulnerability classified as problematic has been found in DedeCMS 5.7.114. This affects an unknown part of the file /sys_verifies.php?action=view. The manipulation of the argument filename with the input ../../../../../etc/passwd leads to path traversal: '../filedir'. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-263889 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-4103	The ADFO – Custom data in admin dashboard plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.9.0. This is due to missing or incorrect nonce validation on several functions hooked via the controller() function. This makes it possible for unauthenticated attackers to edit 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.	4.3	More Details
CVE-2024-4082	The Joli FAQ SEO – WordPress FAQ Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.2. This is due to missing or incorrect nonce validation when saving settings. This makes it possible for unauthenticated attackers to change 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.	4.3	More Details
CVE-2024-4819	A vulnerability was found in Campcodes Online Laundry Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file admin_class.php. The manipulation of the argument type with the input 1 leads to improper authorization. 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-263940.	4.3	More Details
CVE-2024-33942	Missing Authorization vulnerability in Eric Alli Google Typography.This issue affects Google Typography: from n/a through 1.1.2.	4.3	More Details
CVE-2024-4767	If the `browser.privatebrowsing.autostart` preference is enabled, IndexedDB files were not properly deleted when the window was closed. This preference is disabled by default in Firefox. This vulnerability affects Firefox < 126, Firefox ESR < 115.11, and Thunderbird < 115.11.	4.3	More Details
CVE-2024-4561	In WhatsUp Gold versions released before 2023.1.2 , a blind SSRF vulnerability exists in Whatsup Gold's FaviconController that allows an attacker to send arbitrary HTTP requests on behalf of the vulnerable server.	4.2	More Details
CVE-2024-33009	SAP Global Label Management is vulnerable to SQL injection. On exploitation the attacker can use specially crafted inputs to modify database commands resulting in the retrieval of additional information persisted by the system. This could lead to low impact on Confidentiality and Integrity of the application.	4.2	More Details
CVE-2024-4456	In affected versions of Octopus Server with certain access levels it was possible to embed a Cross-Site Scripting payload on the audit page.	4.1	More Details
CVE-2023-52720	Race condition vulnerability in the soundtrigger module Impact: Successful exploitation of this vulnerability will affect availability.	4.1	More Details
CVE-2024-4232	This vulnerability exists in Digisol Router (DG-GR1321: Hardware version 3.7L; Firmware version : v3.2.02) due to lack of encryption or hashing in storing of passwords within the router's firmware/ database. An attacker with physical access could exploit this by extracting the firmware and reverse engineer the binary data to access the plaintext passwords on the vulnerable system. Successful exploitation of this vulnerability could allow the attacker to gain unauthorized access to the targeted system.	4.1	More Details
CVE-2024-22343	IBM TXSeries for Multiplatforms 8.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 280190.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33263	QuickJS commit 3b45d15 was discovered to contain an Assertion Failure via JS_FreeRuntime(JSRuntime *) at quickjs.c.	4.0	More Details
CVE-2024-32020	Git is a revision control system. Prior to versions 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2, and 2.39.4, local clones may end up hardlinking files into the target repository's object database when source and target repository reside on the same disk. If the source repository is owned by a different user, then those hardlinked files may be rewritten at any point in time by the untrusted user. Cloning local repositories will cause Git to either copy or hardlink files of the source repository into the target repository. This significantly speeds up such local clones compared to doing a "proper" clone and saves both disk space and compute time. When cloning a repository located on the same disk that is owned by a different user than the current user we also end up creating such hardlinks. These files will continue to be owned and controlled by the potentially-untrusted user and can be rewritten by them at will in the future. The problem has been patched in versions 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2, and 2.39.4.	3.9	More Details
CVE-2024-32021	Git is a revision control system. Prior to versions 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2, and 2.39.4, when cloning a local source repository that contains symlinks via the filesystem, Git may create hardlinks to arbitrary user-readable files on the same filesystem as the target repository in the `objects/` directory. Cloning a local repository over the filesystem may creating hardlinks to arbitrary user-owned files on the same filesystem in the target Git repository's `objects/` directory. When cloning a repository over the filesystem (without explicitly specifying the `file://` protocol or `--no-local`), the optimizations for local cloning will be used, which include attempting to hard link the object files instead of copying them. While the code includes checks against symbolic links in the source repository, which were added during the fix for CVE-2022-39253, these checks can still be raced because the hard link operation ultimately follows symlinks. If the object on the filesystem appears as a file during the check, and then a symlink during the operation, this will allow the adversary to bypass the check and create hardlinks in the destination objects directory to arbitrary, user-readable files. The problem has been patched in versions 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2, and 2.39.4.	3.9	More Details
CVE-2024-34203	TOTOLINK CP450 v4.1.0cu.747_B20191224 was discovered to contain a stack buffer overflow vulnerability in the setLanguageCfg function.	3.8	More Details
CVE-2024-34218	TOTOLINK outdoor CPE CP450 v4.1.0cu.747_B20191224 was discovered to contain a command injection vulnerability in the NTPSyncWithHost function via the hostTime parameter.	3.8	More Details
CVE-2024-34079	octo-sts is a GitHub App that acts like a Security Token Service (STS) for the Github API. This vulnerability can spike the resource utilization of the STS service, and combined with a significant traffic volume could potentially lead to a denial of service. This vulnerability is fixed in 0.1.0	3.7	More Details
CVE-2024-4855	Use after free issue in editcap could cause denial of service via crafted capture file	3.6	More Details
CVE-2024-4853	Memory handling issue in editcap could cause denial of service via crafted capture file	3.6	More Details
CVE-2024-4686	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /view/emarks_range_grade_update_form.php. The manipulation of the argument grade 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-263627.	3.5	More Details
CVE-2024-4682	A vulnerability has been found in Campcodes Complete Web-Based School Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /view/exam_timetable_update_form.php. The manipulation of the argument exam 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-263623.	3.5	More Details
CVE-2024-4715	A vulnerability, which was classified as problematic, was found in Campcodes Complete Web-Based School Management System 1.0. This affects an unknown part of the file /model/update_grade.php. The manipulation of the argument name 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-263793 was assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4675	A vulnerability has been found in Campcodes Complete Web-Based School Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /view/show_events.php. The manipulation of the argument event_id leads to cross site scripting. 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-263596.	3.5	More Details
CVE-2024-4725	A vulnerability has been found in Campcodes Legal Case Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/client_user. The manipulation of the argument f_name 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-263803.	3.5	More Details
CVE-2024-4724	A vulnerability, which was classified as problematic, was found in Campcodes Legal Case Management System 1.0. Affected is an unknown function of the file /admin/case-type. The manipulation of the argument case_type_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-263802 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-4723	A vulnerability, which was classified as problematic, has been found in Campcodes Legal Case Management System 1.0. This issue affects some unknown processing of the file /admin/case-status. The manipulation of the argument case_status leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-263801 was assigned to this vulnerability.	3.5	More Details
CVE-2024-4722	A vulnerability classified as problematic was found in Campcodes Complete Web-Based School Management System 1.0. This vulnerability affects unknown code of the file index.php. The manipulation of the argument category leads to cross site scripting. 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-263800.	3.5	More Details
CVE-2024-4721	A vulnerability classified as problematic has been found in Campcodes Complete Web-Based School Management System 1.0. This affects an unknown part of the file /model/add_student_subject.php. The manipulation of the argument index 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-263799.	3.5	More Details
CVE-2024-4720	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /model/approve_petty_cash.php. The manipulation of the argument admin_index leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-263798 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-4719	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /model/delete_record.php. The manipulation of the argument page leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-263797 was assigned to this vulnerability.	3.5	More Details
CVE-2024-4676	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /view/range_grade_text.php. The manipulation of the argument count leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-263597 was assigned to this vulnerability.	3.5	More Details
CVE-2024-4649	A vulnerability classified as problematic has been found in Campcodes Complete Web-Based School Management System 1.0. This affects an unknown part of the file /view/student_exam_mark_insert_form1.php. The manipulation of the argument page 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-263493 was assigned to this vulnerability.	3.5	More Details
CVE-2024-4677	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file /view/my_student_exam_marks1.php. The manipulation of the argument year 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-263598 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-4678	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /view/find_friends.php. The manipulation of the argument my_type 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-263599.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4683	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /view/exam_timetable_insert_form.php. The manipulation of the argument exam leads to cross site scripting. 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-263624.	3.5	More Details
CVE-2024-4674	A vulnerability, which was classified as problematic, was found in Campcodes Complete Web-Based School Management System 1.0. This affects an unknown part of the file /view/show_friend_request.php. The manipulation of the argument my_index 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-263595.	3.5	More Details
CVE-2024-4684	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /view/exam_timetable_grade_wise.php. The manipulation of the argument exam 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-263625 was assigned to this vulnerability.	3.5	More Details
CVE-2024-4685	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /view/exam_timetable.php. The manipulation of the argument exam leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-263626 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-4650	A vulnerability classified as problematic was found in Campcodes Complete Web-Based School Management System 1.0. This vulnerability affects unknown code of the file /view/student_due_payment.php. The manipulation of the argument due_month leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-263494 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-4687	A vulnerability classified as problematic has been found in Campcodes Complete Web-Based School Management System 1.0. Affected is an unknown function of the file /view/create_events.php. The manipulation of the argument my_index leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-263628.	3.5	More Details
CVE-2024-4651	A vulnerability, which was classified as problematic, has been found in Campcodes Complete Web-Based School Management System 1.0. This issue affects some unknown processing of the file /view/student_attendance_history1.php. The manipulation of the argument year 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-263495.	3.5	More Details
CVE-2024-4652	A vulnerability, which was classified as problematic, was found in Campcodes Complete Web-Based School Management System 1.0. Affected is an unknown function of the file /view/show_teacher2.php. The manipulation of the argument month leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-263496.	3.5	More Details
CVE-2024-4688	A vulnerability classified as problematic was found in Campcodes Complete Web-Based School Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /view/conversation_history_admin.php. The manipulation of the argument conversation_id leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-263629 was assigned to this vulnerability.	3.5	More Details
CVE-2024-4713	A vulnerability classified as problematic was found in Campcodes Complete Web-Based School Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /view/all_teacher.php. The manipulation of the argument page 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-263791.	3.5	More Details
CVE-2024-4714	A vulnerability, which was classified as problematic, has been found in Campcodes Complete Web-Based School Management System 1.0. Affected by this issue is some unknown functionality of the file /model/update_subject.php. The manipulation of the argument name leads to cross site scripting. 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-263792.	3.5	More Details
CVE-2024-4718	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file /model/delete_student_grade_subject.php. The manipulation of the argument index leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-263796.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4717	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /model/update_classroom.php. The manipulation of the argument name 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-263795.	3.5	More Details
CVE-2024-28971	Dell Update Manager Plugin, versions 1.4.0 through 1.5.0, contains a Plain-text Password Storage Vulnerability in Log file. A remote high privileged attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	3.5	More Details
CVE-2024-4726	A vulnerability was found in Campcodes Legal Case Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/clients. The manipulation of the argument f_name leads to cross site scripting. 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-263804.	3.5	More Details
CVE-2024-4716	A vulnerability has been found in Campcodes Complete Web-Based School Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /model/update_exam.php. The manipulation of the argument name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-263794 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-4673	A vulnerability, which was classified as problematic, has been found in Campcodes Complete Web-Based School Management System 1.0. Affected by this issue is some unknown functionality of the file /view/show_student_grade_subject.php. The manipulation of the argument id leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-263594 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-4729	A vulnerability was found in Campcodes Legal Case Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/expense-type. The manipulation of the argument name 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-263807.	3.5	More Details
CVE-2024-34713	sshproxy is used on a gateway to transparently proxy a user SSH connection on the gateway to an internal host via SSH. Prior to version 1.6.3, any user authorized to connect to a ssh server using `sshproxy` can inject options to the `ssh` command executed by `sshproxy`. All versions of `sshproxy` are impacted. The problem is patched starting in version 1.6.3. The only workaround is to use the `force_command` option in `sshproxy.yaml`, but it's rarely relevant.	3.5	More Details
CVE-2024-34355	TYPO3 is an enterprise content management system. Starting in version 13.0.0 and prior to version 13.1.1, the history backend module is vulnerable to HTML injection. Although Content-Security-Policy headers effectively prevent JavaScript execution, adversaries can still inject malicious HTML markup. Exploiting this vulnerability requires a valid backend user account. TYPO3 version 13.1.1 fixes the problem described.	3.5	More Details
CVE-2024-4797	A vulnerability was found in Campcodes Online Laundry Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /ajax.php. The manipulation of the argument name/customer_name/username leads to cross site scripting. 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-263896.	3.5	More Details
CVE-2024-4738	A vulnerability was found in Campcodes Legal Case Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument new_client leads to cross site scripting. 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-263824.	3.5	More Details
CVE-2024-4737	A vulnerability was found in Campcodes Legal Case Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /admin/vendor. The manipulation of the argument company_name/mobile 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-263823.	3.5	More Details
CVE-2024-4736	A vulnerability was found in Campcodes Legal Case Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/tax. The manipulation of the argument name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-263822 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4735	A vulnerability has been found in Campcodes Legal Case Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/tasks. The manipulation of the argument task_subject leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-263821 was assigned to this vulnerability.	3.5	More Details
CVE-2024-4732	A vulnerability, which was classified as problematic, has been found in Campcodes Legal Case Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/service. The manipulation of the argument name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-263810 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-33007	PDFViewer is a control delivered as part of SAPUI5 product which shows the PDF content in an embedded mode by default. If a PDF document contains embedded JavaScript (or any harmful client-side script), the PDFViewer will execute the JavaScript embedded in the PDF which can cause a potential security threat.	3.5	More Details
CVE-2024-33000	SAP Bank Account Management does not perform necessary authorization check for an authorized user, resulting in escalation of privileges. As a result, it has a low impact to confidentiality to the system.	3.5	More Details
CVE-2024-4730	A vulnerability classified as problematic has been found in Campcodes Legal Case Management System 1.0. Affected is an unknown function of the file /admin/judge. The manipulation of the argument judge_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. The identifier of this vulnerability is VDB-263808.	3.5	More Details
CVE-2024-4731	A vulnerability classified as problematic was found in Campcodes Legal Case Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/role. The manipulation of the argument slug leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-263809 was assigned to this vulnerability.	3.5	More Details
CVE-2024-4646	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file /view/student_payment_details.php. The manipulation of the argument index 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-263490 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-4672	A vulnerability classified as problematic was found in Campcodes Complete Web-Based School Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /view/show_student_subject.php. The manipulation of the argument id leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-263593 was assigned to this vulnerability.	3.5	More Details
CVE-2024-4727	A vulnerability was found in Campcodes Legal Case Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /admin/court-type. The manipulation of the argument court_name 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-263805 was assigned to this vulnerability.	3.5	More Details
CVE-2024-4648	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /view/student_exam_mark_update_form.php. The manipulation of the argument std_index leads to cross site scripting. 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-263492.	3.5	More Details
CVE-2024-4645	A vulnerability was found in SourceCodester Prison Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /Admin/changepassword.php. The manipulation of the argument txtold_password/txtnew_password/txtconfirm_password leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-263489 was assigned to this vulnerability.	3.5	More Details
CVE-2024-4728	A vulnerability was found in Campcodes Legal Case Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/court. The manipulation of the argument court_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-263806 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4647	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /view/student_first_payment.php. The manipulation of the argument index 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-263491.	3.5	More Details
CVE-2024-4644	A vulnerability has been found in SourceCodester Prison Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /Employee/changepassword.php. The manipulation of the argument txtold_password/txtnew_password/txtconfirm_password leads to cross site scripting. 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-263488.	3.5	More Details
CVE-2024-33583	A vulnerability has been identified in SIMATIC RTLS Locating Manager (6GT2780-0DA00) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-0DA30) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA10) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA20) (All versions < V3.0.1.1), SIMATIC RTLS Locating Manager (6GT2780-1EA30) (All versions < V3.0.1.1). Affected application contains a hidden configuration item to enable debug functionality. This could allow an authenticated local attacker to gain insight into the internal configuration of the deployment.	3.3	More Details
CVE-2024-27837	A downgrade issue was addressed with additional code-signing restrictions. This issue is fixed in macOS Sonoma 14.5. A local attacker may gain access to Keychain items.	3.3	More Details
CVE-2024-32989	Insufficient verification vulnerability in the system sharing pop-up module Impact: Successful exploitation of this vulnerability will affect availability.	3.3	More Details
CVE-2024-27839	A privacy issue was addressed by moving sensitive data to a more secure location. This issue is fixed in iOS 17.5 and iPadOS 17.5. A malicious application may be able to determine a user's current location.	3.3	More Details
CVE-2024-32637	A vulnerability has been identified in JT2Go (All versions < V2312.0005), Teamcenter Visualization V14.2 (All versions < V14.2.0.12), Teamcenter Visualization V14.3 (All versions < V14.3.0.10), Teamcenter Visualization V2312 (All versions < V2312.0005). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted X_T files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	3.3	More Details
CVE-2024-4317	Missing authorization in PostgreSQL built-in views pg_stats_ext and pg_stats_ext_exprs allows an unprivileged database user to read most common values and other statistics from CREATE STATISTICS commands of other users. The most common values may reveal column values the eavesdropper could not otherwise read or results of functions they cannot execute. Installing an unaffected version only fixes fresh PostgreSQL installations, namely those that are created with the initdb utility after installing that version. Current PostgreSQL installations will remain vulnerable until they follow the instructions in the release notes. Within major versions 14-16, minor versions before PostgreSQL 16.3, 15.7, and 14.12 are affected. Versions before PostgreSQL 14 are unaffected.	3.1	More Details
CVE-2024-28866	GoCD is a continuous delivery server. GoCD versions from 19.4.0 to 23.5.0 (inclusive) are potentially vulnerable to a reflected cross-site scripting vulnerability on the loading page displayed while GoCD is starting, via abuse of a `redirect_to` query parameter with inadequate validation. Attackers could theoretically abuse the query parameter to steal session tokens or other values from the user's browser. In practice exploiting this to perform privileged actions is likely rather difficult to exploit because the target user would need to be triggered to open an attacker-crafted link in the period where the server is starting up (but not completely started), requiring chaining with a separate denial-of-service vulnerability. Additionally, GoCD server restarts invalidate earlier session tokens (i.e GoCD does not support persistent sessions), so a stolen session token would be unusable once the server has completed restart, and executed XSS would be done within a logged-out context. The issue is fixed in GoCD 24.1.0. As a workaround, it is technically possible in earlier GoCD versions to override the loading page with an earlier version which is not vulnerable, by starting GoCD with the Java system property override as either `-Dloading.page.resource.path=/loading_pages/default.loading.page.html` (simpler early version of loading page without GoCD introduction) or `-Dloading.page.resource.path=/does_not_exist.html` (to display a simple message with no interactivity).	3.1	More Details
CVE-2023-47711	IBM Security Guardium 11.3, 11.4, 11.5, and 12.0 could allow an authenticated user to upload files that would cause a denial of service. IBM X-Force ID: 271526.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27803	A permissions issue was addressed with improved validation. This issue is fixed in iOS 17.5 and iPadOS 17.5. An attacker with physical access may be able to share items from the lock screen.	2.4	More Details
CVE-2024-27835	This issue was addressed through improved state management. This issue is fixed in iOS 17.5 and iPadOS 17.5. An attacker with physical access to an iOS device may be able to access notes from the lock screen.	2.4	More Details
CVE-2024-22460	Dell PowerProtect DM5500 version 5.15.0.0 and prior contains an insecure deserialization Vulnerability. A remote attacker with high privileges could potentially exploit this vulnerability, leading to arbitrary code execution on the vulnerable application.	2.2	More Details
CVE-2024-4774	The `ShmemCharMapHashEntry()` code was susceptible to potentially undefined behavior by bypassing the move semantics for one of its data members. This vulnerability affects Firefox < 126.	N/A	More Details
CVE-2024-26579	Deserialization of Untrusted Data vulnerability in Apache InLong.This issue affects Apache InLong: from 1.7.0 through 1.11.0, the attackers can bypass using malicious parameters. Users are advised to upgrade to Apache InLong's 1.12.0 or cherry-pick [1], [2] to solve it. [1] https://github.com/apache/inlong/pull/9694 [2] https://github.com/apache/inlong/pull/9707	N/A	More Details
CVE-2024-1076	The SSL Zen WordPress plugin before 4.6.0 does not properly prevent directory listing of the private keys folder, as it only relies on the use of .htaccess to prevent visitors from accessing the site's generated private keys, which allows an attacker to read them if the site runs on a server who doesn't support .htaccess files, like NGINX.	N/A	More Details
CVE-2024-4777	Memory safety bugs present in Firefox 125, Firefox ESR 115.10, and Thunderbird 115.10. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 126, Firefox ESR < 115.11, and Thunderbird < 115.11.	N/A	More Details
CVE-2024-4810	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. This CVE has been replaced by CVE-2024-36015.	N/A	More Details
CVE-2024-25527	RuvarOA v6.01 and v12.01 were discovered to contain a SQL injection vulnerability via the id parameter at /PersonalAffair/worklog_template_show.aspx.	N/A	More Details
CVE-2024-31810	TOTOLINK EX200 V4.0.3c.7646_B20201211 was discovered to contain a hardcoded password for root at /etc/shadow.sample.	N/A	More Details
CVE-2024-4614	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-2299	A stored Cross-Site Scripting (XSS) vulnerability exists in the parisneo/lollms-webui application due to improper validation of uploaded files in the profile picture upload functionality. Attackers can exploit this vulnerability by uploading malicious HTML files containing JavaScript code, which is executed when the file is accessed. This vulnerability is remotely exploitable via Cross-Site Request Forgery (CSRF), allowing attackers to perform actions on behalf of authenticated users and potentially leading to unauthorized access to sensitive information within the Lollms-webui application.	N/A	More Details
CVE-2024-2441	The VikBooking Hotel Booking Engine & PMS WordPress plugin before 1.6.8 allows direct access to menus, allowing an authenticated user with subscriber privileges or above, to bypass authorization and access settings of the VikBooking Hotel Booking Engine & PMS WordPress plugin before 1.6.8's they shouldn't be allowed to.	N/A	More Details
CVE-2024-4579	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-4295. Reason: This candidate is a reservation duplicate of CVE-2024-4295. Notes: All CVE users should reference CVE-2024-4295 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-4572	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: 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-2024-4571	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-4542	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-3548. Reason: This candidate was issued in error. Please use CVE-2024-3548 instead.	N/A	More Details
CVE-2024-4424	The access control in CemiPark software does not properly validate user-entered data, which allows the stored cross-site scripting (XSS) attack. The parameters used to enter data into the system do not have appropriate validation, which makes possible to smuggle in HTML/JavaScript code. This code will be executed in the user's browser space.This issue affects CemiPark software: 4.5, 4.7, 5.03 and potentially others. The vendor refused to provide the specific range of affected products.	N/A	More Details
CVE-2024-4367	A type check was missing when handling fonts in PDF.js, which would allow arbitrary JavaScript execution in the PDF.js context. This vulnerability affects Firefox < 126, Firefox ESR < 115.11, and Thunderbird < 115.11.	N/A	More Details
CVE-2024-33386	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2024-3941	The reCAPTCHA Jetpack WordPress plugin through 0.2.2 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged-in admin add Stored XSS payloads via a CSRF attack.	N/A	More Details
CVE-2024-33818	Globitel KSA SpeechLog v8.1 was discovered to contain an Insecure Direct Object Reference (IDOR) via the userID parameter.	N/A	More Details
CVE-2024-3940	The reCAPTCHA Jetpack WordPress plugin through 0.2.2 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	N/A	More Details
CVE-2024-33878	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2024-34243	Konga v0.14.9 is vulnerable to Cross Site Scripting (XSS) via the username parameter.	N/A	More Details
CVE-2024-3582	The UnGallery WordPress plugin through 2.2.4 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	N/A	More Details
CVE-2024-29212	Due to an unsafe de-serialization method used by the Veeam Service Provider Console(VSPC) server in communication between the management agent and its components, under certain conditions, it is possible to perform Remote Code Execution (RCE) on the VSPC server machine.	N/A	More Details
CVE-2024-4631	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-3557. Reason: This candidate was issued in error and is a duplicate. Please use CVE-2024-3557 instead. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-28277	In Sourcecodester School Task Manager v1.0, a vulnerability was identified within the subject_name= parameter, enabling Stored Cross-Site Scripting (XSS) attacks. This vulnerability allows attackers to manipulate the subject's name, potentially leading to the execution of malicious JavaScript payloads.	N/A	More Details
CVE-2024-27401	In the Linux kernel, the following vulnerability has been resolved: firewire: nosy: ensure user_length is taken into account when fetching packet contents Ensure that packet_buffer_get respects the user_length provided. If the length of the head packet exceeds the user_length, packet_buffer_get will now return 0 to signify to the user that no data were read and a larger buffer size is required. Helps prevent user space overflows.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33382	An issue in Open5GS v.2.7.0 allows an attacker to cause a denial of service via the 64 unsuccessful UE/gnb registration	N/A	More Details
CVE-2020-36662	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-26863	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-52654	In the Linux kernel, the following vulnerability has been resolved: io_uring/af_unix: disable sending io_uring over sockets File reference cycles have caused lots of problems for io_uring in the past, and it still doesn't work exactly right and races with unix_stream_read_generic(). The safest fix would be to completely disallow sending io_uring files via sockets via SCM_RIGHT, so there are no possible cycles invloving registered files and thus rendering SCM accounting on the io_uring side unnecessary.	N/A	More Details
CVE-2023-52655	In the Linux kernel, the following vulnerability has been resolved: usb: aqc111: check packet for fixup for true limit If a device sends a packet that is inbetween 0 and sizeof(u64) the value passed to skb_trim() as length will wrap around ending up as some very large value. The driver will then proceed to parse the header located at that position, which will either oops or process some random value. The fix is to check against sizeof(u64) rather than 0, which the driver currently does. The issue exists since the introduction of the driver.	N/A	More Details
CVE-2023-52656	In the Linux kernel, the following vulnerability has been resolved: io_uring: drop any code related to SCM_RIGHTS This is dead code after we dropped support for passing io_uring fds over SCM_RIGHTS, get rid of it.	N/A	More Details
CVE-2024-34899	WWBN AVideo 12.4 is vulnerable to Cross Site Scripting (XSS).	N/A	More Details
CVE-2024-24157	Gnuboard g6 / https://github.com/gnuboard/g6 commit c2cc1f5069e00491ea48618d957332d90f6d40e4 is vulnerable to Cross Site Scripting (XSS) via board.py.	N/A	More Details
CVE-2024-26306	iPerf3 before 3.17, when used with OpenSSL before 3.2.0 as a server with RSA authentication, allows a timing side channel in RSA decryption operations. This side channel could be sufficient for an attacker to recover credential plaintext. It requires the attacker to send a large number of messages for decryption, as described in "Everlasting ROBOT: the Marvin Attack" by Hubert Kario.	N/A	More Details
CVE-2024-27395	In the Linux kernel, the following vulnerability has been resolved: net: openvswitch: Fix Use-After-Free in ovs_ct_exit Since kfree_rcu, which is called in the hlist_for_each_entry_rcu traversal of ovs_ct_limit_exit, is not part of the RCU read critical section, it is possible that the RCU grace period will pass during the traversal and the key will be free. To prevent this, it should be changed to hlist_for_each_entry_safe.	N/A	More Details
CVE-2024-27396	In the Linux kernel, the following vulnerability has been resolved: net: gtp: Fix Use-After-Free in gtp_dellink Since call_rcu, which is called in the hlist_for_each_entry_rcu traversal of gtp_dellink, is not part of the RCU read critical section, it is possible that the RCU grace period will pass during the traversal and the key will be free. To prevent this, it should be changed to hlist_for_each_entry_safe.	N/A	More Details
CVE-2024-27397	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: use timestamp to check for set element timeout Add a timestamp field at the beginning of the transaction, store it in the nftables per-netns area. Update set backend .insert, .deactivate and sync gc path to use the timestamp, this avoids that an element expires while control plane transaction is still unfinished. .lookup and .update, which are used from packet path, still use the current time to check if the element has expired. And .get path and dump also since this runs lockless under rcu read size lock. Then, there is async gc which also needs to check the current time since it runs asynchronously from a workqueue.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27398	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: Fix use-after-free bugs caused by sco_sock_timeout When the sco connection is established and then, the sco socket is releasing, timeout_work will be scheduled to judge whether the sco disconnection is timeout. The sock will be deallocated later, but it is dereferenced again in sco_sock_timeout. As a result, the use-after-free bugs will happen. The root cause is shown below: Cleanup Thread | Worker Thread sco_sock_release | sco_sock_close | __sco_sock_close | sco_sock_set_timer | schedule_delayed_work | sco_sock_kill | (wait a time) sock_put(sk) //FREE | sco_sock_timeout | sock_hold(sk) //USE The KASAN report triggered by POC is shown below: [95.890016] == [95.890496] BUG: KASAN: slab-use-after-free in sco_sock_timeout+0x5e/0x1c0 [95.890755] Write of size 4 at addr ffff88800c388080 by task kworker/0:0/7 ... [95.890755] Workqueue: events sco_sock_timeout [95.890755] Call Trace: [95.890755] <TASK> [95.890755] dump_stack_lvl+0x45/0x110 [95.890755] print_address_description+0x78/0x390 [95.890755] print_report+0x11b/0x250 [95.890755] ? __virt_addr_valid+0xbe/0xf0 [95.890755] ? sco_sock_timeout+0x5e/0x1c0 [95.890755] kasan_report+0x139/0x170 [95.890755] ? update_load_avg+0xe5/0x9f0 [95.890755] ? sco_sock_timeout+0x5e/0x1c0 [95.890755] kasan_check_range+0x2c3/0x2e0 [95.890755] sco_sock_timeout+0x5e/0x1c0 [95.890755] process_one_work+0x561/0xc50 [95.890755] worker_thread+0xab2/0x13c0 [95.890755] ? pr_cont_work+0x490/0x490 [95.890755] kthread+0x279/0x300 [95.890755] ? pr_cont_work+0x490/0x490 [95.890755] ? kthread_blkcg+0xa0/0xa0 [95.890755] ret_from_fork+0x34/0x60 [95.890755] ? kthread_blkcg+0xa0/0xa0 [95.890755] ret_from_fork_asm+0x11/0x20 [95.890755] </TASK> [95.890755] [95.890755] Allocated by task 506: [95.890755] kasan_save_track+0x3f/0x70 [95.890755] __kasan_kmalloc+0x86/0x90 [95.890755] __kmalloc+0x17f/0x360 [95.890755] sk_prot_alloc+0xe1/0x1a0 [95.890755] sk_alloc+0x31/0x4e0 [95.890755] bt_sock_alloc+0x2b/0x2a0 [95.890755] sco_sock_create+0xad/0x320 [95.890755] bt_sock_create+0x145/0x320 [95.890755] __sock_create+0x2e1/0x650 [95.890755] __sys_socket+0xd0/0x280 [95.890755] __x64_sys_socket+0x75/0x80 [95.890755] do_syscall_64+0xc4/0x1b0 [95.890755] entry_SYSCALL_64_after_hwframe+0x67/0x6f [95.890755] [95.890755] Freed by task 506: [95.890755] kasan_save_track+0x3f/0x70 [95.890755] kasan_save_free_info+0x40/0x50 [95.890755] poison_slab_object+0x118/0x180 [95.890755] __kasan_slab_free+0x12/0x30 [95.890755] kfree+0xb2/0x240 [95.890755] __sk_destruct+0x317/0x410 [95.890755] sco_sock_release+0x232/0x280 [95.890755] sock_close+0xb2/0x210 [95.890755] __fput+0x37f/0x770 [95.890755] task_work_run+0x1ae/0x210 [95.890755] get_signal+0xe17/0xf70 [95.890755] arch_do_signal_or_restart+0x3f/0x520 [95.890755] syscall_exit_to_user_mode+0x55/0x120 [95.890755] do_syscall_64+0xd1/0x1b0 [95.890755] entry_SYSCALL_64_after_hwframe+0x67/0x6f [95.890755] [95.890755] The buggy address belongs to the object at ffff88800c388000 [95.890755] which belongs to the cache kmalloc-1k of size 1024 [95.890755] The buggy address is located 128 bytes inside of [95.890755] freed 1024-byte region [ffff88800c388000, ffff88800c388400) [95.890755] [95.890755] The buggy address belongs to the physical page: [95.890755] page: refcount:1 mapcount:0 mapping:0000000000000000 index:0xffff88800c38a800 pfn:0xc388 [95.890755] head: order:3 entire_mapcount:0 nr_pages_mapped:0 pincount:0 [95.890755] ano ---truncated---	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27399	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: l2cap: fix null-ptr-deref in l2cap_chan_timeout There is a race condition between l2cap_chan_timeout() and l2cap_chan_del(). When we use l2cap_chan_del() to delete the channel, the chan->conn will be set to null. But the conn could be dereferenced again in the mutex_lock() of l2cap_chan_timeout(). As a result the null pointer dereference bug will happen. The KASAN report triggered by POC is shown below: [472.074580] == [472.075284] BUG: KASAN: null-ptr-deref in mutex_lock+0x68/0xc0 [472.075308] Write of size 8 at addr 0000000000000158 by task kworker/0:0/7 [472.075308] [472.075308] CPU: 0 PID: 7 Comm: kworker/0:0 Not tainted 6.9.0-rc5-00356-g78c0094a146b #36 [472.075308] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-prebuilt.qemu4 [472.075308] Workqueue: events l2cap_chan_timeout [472.075308] Call Trace: [472.075308] <TASK> [472.075308] dump_stack_lvl+0x137/0x1a0 [472.075308] print_report+0x101/0x250 [472.075308] ? __virt_addr_valid+0x77/0x160 [472.075308] ? mutex_lock+0x68/0xc0 [472.075308] kasan_report+0x139/0x170 [472.075308] ? mutex_lock+0x68/0xc0 [472.075308] kasan_check_range+0x2c3/0x2e0 [472.075308] mutex_lock+0x68/0xc0 [472.075308] l2cap_chan_timeout+0x181/0x300 [472.075308] process_one_work+0x5d2/0xe00 [472.075308] worker_thread+0xe1d/0x1660 [472.075308] ? pr_cont_work+0x5e0/0x5e0 [472.075308] kthread+0x2b7/0x350 [472.075308] ? pr_cont_work+0x5e0/0x5e0 [472.075308] ? kthread_blkcg+0xd0/0xd0 [472.075308] ret_from_fork+0x4d/0x80 [472.075308] ? kthread_blkcg+0xd0/0xd0 [472.075308] ret_from_fork_asm+0x11/0x20 [472.075308] </TASK> [472.075308] == [472.094860] Disabling lock debugging due to kernel taint [472.096136] BUG: kernel NULL pointer dereference, address: 0000000000000158 [472.096136] #PF: supervisor write access in kernel mode [472.096136] #PF: error_code(0x0002) - not-present page [472.096136] PGD 0 P4D 0 [472.096136] Oops: 0002 [#1] PREEMPT SMP KASAN NOPTI [472.096136] CPU: 0 PID: 7 Comm: kworker/0:0 Tainted: G B 6.9.0-rc5-00356-g78c0094a146b #36 [472.096136] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.14.0-0-g155821a1990b-prebuilt.qemu4 [472.096136] Workqueue: events l2cap_chan_timeout [472.096136] RIP: 0010:mutex_lock+0x88/0xc0 [472.096136] Code: be 08 00 00 00 e8 f8 23 1f fd 4c 89 f7 be 08 00 00 00 e8 eb 23 1f fd 42 80 3c 23 00 74 08 48 88 [472.096136] RSP: 0018:ffff88800744fc78 EFLAGS: 00000246 [472.096136] RAX: 0000000000000000 RBX: 1ffff11000e89f8f RCX: ffffffff8457c865 [472.096136] RDX: 0000000000000001 RSI: 0000000000000008 RDI: ffff88800744fc78 [472.096136] RBP: 0000000000000158 R08: ffff88800744fc7f R09: 1ffff11000e89f8f [472.096136] R10: dfffc0000000000 R11: ffffed1000e89f90 R12: dfffc0000000000 [472.096136] R13: 0000000000000158 R14: ffff88800744fc78 R15: ffff888007405a00 [472.096136] FS: 0000000000000000(0000) GS:ffff88806d200000(0000) knlGS:0000000000000000 [472.096136] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [472.096136] CR2: 0000000000000158 CR3: 000000000da32000 CR4: 00000000000006f0 [472.096136] Call Trace: [472.096136] <TASK> [472.096136] ? __die_body+0x8d/0xe0 [472.096136] ? page_fault_oops+0x6b8/0x9a0 [472.096136] ? kernelmode_fixup_or_oops+0x20c/0x2a0 [472.096136] ? do_user_addr_fault+0x1027/0x1340 [472.096136] ? _printk+0x7a/0xa0 [472.096136] ? mutex_lock+0x68/0xc0 [472.096136] ? add_taint+0x42/0xd0 [472.096136] ? exc_page_fault+0x6a/0x1b0 [472.096136] ? asm_exc_page_fault+0x26/0x30 [472.096136] ? mutex_lock+0x75/0xc0 [472.096136] ? mutex_lock+0x88/0xc0 [472.096136] ? mutex_lock+0x75/0xc0 [472.096136] l2cap_chan_timeo ---truncated---	N/A	More Details
CVE-2024-27400	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: once more fix the call oder in amdgpu_ttm_move() v2 This reverts drm/amdgpu: fix ftrace event amdgpu_bo_move always move on same heap. The basic problem here is that after the move the old location is simply not available any more. Some fixes were suggested, but essentially we should call the move notification before actually moving things because only this way we have the correct order for DMA-buf and VM move notifications as well. Also rework the statistic handling so that we don't update the eviction counter before the move. v2: add missing NULL check	N/A	More Details
CVE-2024-34749	Phormer prior to version 3.35 contains a cross-site scripting vulnerability. If this vulnerability is exploited, a remote unauthenticated attacker may execute an arbitrary script on the web browser of the user.	N/A	More Details