SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 24 July 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-2024-40628	JumpServer is an open-source Privileged Access Management (PAM) tool that provides DevOps and IT teams with on-demand and secure access to SSH, RDP, Kubernetes, Database and RemoteApp endpoints through a web browser. An attacker can exploit the ansible playbook to read arbitrary files in the celery container, leading to sensitive information disclosure. The Celery container runs as root and has database access, allowing the attacker to steal all secrets for hosts, create a new JumpServer account with admin privileges, or manipulate the database in other ways. This issue has been addressed in release versions 3.10.12 and 4.0.0. It is recommended to upgrade the safe versions. There is no known workarounds for this vulnerability.	10.0	More Details
CVE-2024-40629	JumpServer is an open-source Privileged Access Management (PAM) tool that provides DevOps and IT teams with on-demand and secure access to SSH, RDP, Kubernetes, Database and RemoteApp endpoints through a web browser. An attacker can exploit the Ansible playbook to write arbitrary files, leading to remote code execution (RCE) in the Celery container. The Celery container runs as root and has database access, allowing an attacker to steal all secrets for hosts, create a new JumpServer account with admin privileges, or manipulate the database in other ways. This issue has been patched in release versions 3.10.12 and 4.0.0. It is recommended to upgrade the safe versions. There are no known workarounds for this vulnerability.	10.0	More Details
CVE-2024-39911	1Panel is a web-based linux server management control panel. 1Panel contains an unspecified sql injection via User-Agent handling. This issue has been addressed in version 1.10.12-lts. Users are advised to upgrade. There are no known workarounds for this vulnerability.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20419	A vulnerability in the authentication system of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an unauthenticated, remote attacker to change the password of any user, including administrative users. This vulnerability is due to improper implementation of the password-change process. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow an attacker to access the web UI or API with the privileges of the compromised user.	10.0	More Details
CVE-2024-5618	Incorrect Permission Assignment for Critical Resource vulnerability in PruvaSoft Informatics Apinizer Management Console allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Apinizer Management Console: before 2024.05.1.	9.9	More Details
CVE-2024-41703	LibreChat through 0.7.4-rc1 has incorrect access control for message updates.	9.8	More Details
CVE-2024-38438	D-Link - CWE-294: Authentication Bypass by Capture-replay	9.8	More Details
CVE-2024-38437	D-Link - CWE-288:Authentication Bypass Using an Alternate Path or Channel	9.8	More Details
CVE-2024-6636	The WooCommerce - Social Login plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'woo_slg_login_email' function in all versions up to, and including, 2.7.3. This makes it possible for unauthenticated attackers to change the default role to Administrator while registering for an account.	9.8	More Details
CVE-2024-41704	LibreChat through 0.7.4-rc1 does not validate the normalized pathnames of images.	9.8	More Details
CVE-2024-39685	Bert-VITS2 is the VITS2 Backbone with multilingual bert. User input supplied to the data_dir variable is used directly in a command executed with subprocess.run(cmd, shell=True) in the resample function, which leads to arbitrary command execution. This affects fishaudio/Bert-VITS2 2.3 and earlier.	9.8	More Details
CVE-2024-6205	The PayPlus Payment Gateway WordPress plugin before 6.6.9 does not properly sanitise and escape a parameter before using it in a SQL statement via a WooCommerce API route available to unauthenticated users, leading to an SQL injection vulnerability.	9.8	More Details
CVE-2024-35198	TorchServe is a flexible and easy-to-use tool for serving and scaling PyTorch models in production. TorchServe 's check on allowed_urls configuration can be by-passed if the URL contains characters such as ".." but it does not prevent the model from being downloaded into the model store. Once a file is downloaded, it can be referenced without providing a URL the second time, which effectively bypasses the allowed_urls security check. Customers using PyTorch inference Deep Learning Containers (DLC) through Amazon SageMaker and EKS are not affected. This issue in TorchServe has been fixed by validating the URL without characters such as ".." before downloading see PR #3082. TorchServe release 0.11.0 includes the fix to address this vulnerability. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.8	More Details
CVE-2024-21552	All versions of `SuperAGI` are vulnerable to Arbitrary Code Execution due to unsafe use of the ‘eval’ function. An attacker could induce the LLM output to exploit this vulnerability and gain arbitrary code execution on the SuperAGI application server.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39173	calculator-boilerplate v1.0 was discovered to contain a remote code execution (RCE) vulnerability via the eval function at /routes/calculator.js. This vulnerability allows attackers to execute arbitrary code via a crafted payload injected into the input field.	9.8	More Details
CVE-2024-0857	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Universal Software Inc. FlexWater Corporate Water Management allows SQL Injection.This issue affects FlexWater Corporate Water Management: before 5.452.0.	9.8	More Details
CVE-2024-39686	Bert-VITS2 is the VITS2 Backbone with multilingual bert. User input supplied to the data_dir variable is used directly in a command executed with subprocess.run(cmd, shell=True) in the bert_gen function, which leads to arbitrary command execution. This affects fishaudio/Bert-VITS2 2.3 and earlier.	9.8	More Details
CVE-2024-37998	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V5.40), SICORE Base system (All versions < V1.4.0). The password of administrative accounts of the affected applications can be reset without requiring the knowledge of the current password, given the auto login is enabled. This could allow an unauthorized attacker to obtain administrative access of the affected applications.	9.8	More Details
CVE-2024-39962	D-Link DIR-823X AX3000 Dual-Band Gigabit Wireless Router v21_D240126 was discovered to contain a remote code execution (RCE) vulnerability in the ntp_zone_val parameter at /goform/set_ntp. This vulnerability is exploited via a crafted HTTP request.	9.8	More Details
CVE-2024-6220	The 简数采集器 (Keydatas) plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the keydatas_downloadImages function in all versions up to, and including, 2.5.2. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2024-41318	TOTOLINK A6000R V1.0.1-B20201211.2000 was discovered to contain a command injection vulnerability via the ifname parameter in the apcli_wps_gen_pincode function.	9.8	More Details
CVE-2024-40502	SQL injection vulnerability in Hospital Management System Project in ASP.Net MVC 1 allows aremote attacker to execute arbitrary code via the btn_login_b_Click function of the Loginpage.aspx	9.8	More Details
CVE-2024-36491	FutureNet NXR series, VXR series and WXR series provided by Century Systems Co., Ltd. allow a remote unauthenticated attacker to execute an arbitrary OS command, obtain and/or alter sensitive information, and be able to cause a denial of service (DoS) condition.	9.8	More Details
CVE-2024-41319	TOTOLINK A6000R V1.0.1-B20201211.2000 was discovered to contain a command injection vulnerability via the cmd parameter in the webcmd function.	9.8	More Details
CVE-2024-6912	Use of hard-coded MSSQL credentials in PerkinElmer ProcessPlus on Windows allows an attacker to login remove on all prone installations.This issue affects ProcessPlus: through 1.11.6507.0.	9.8	More Details
CVE-2024-6806	The NI VeriStand Gateway is missing authorization checks when an actor attempts to access Project resources. These missing checks may result in remote code execution. This affects NI VeriStand 2024 Q2 and prior versions.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6794	A deserialization of untrusted data vulnerability exists in NI VeriStand Waveform Streaming Server that may result in remote code execution. Successful exploitation requires an attacker to send a specially crafted message. These vulnerabilities affect NI VeriStand 2024 Q2 and prior versions.	9.8	More Details
CVE-2024-6793	A deserialization of untrusted data vulnerability exists in NI VeriStand DataLogging Server that may result in remote code execution. Successful exploitation requires an attacker to send a specially crafted message. These vulnerabilities affect NI VeriStand 2024 Q2 and prior versions.	9.8	More Details
CVE-2024-41316	TOTOLINK A6000R V1.0.1-B20201211.2000 was discovered to contain a command injection vulnerability via the ifname parameter in the apcli_cancel_wps function.	9.8	More Details
CVE-2024-39907	1Panel is a web-based linux server management control panel. There are many sql injections in the project, and some of them are not well filtered, leading to arbitrary file writes, and ultimately leading to RCEs. These sql injections have been resolved in version 1.10.12-tls. Users are advised to upgrade. There are no known workarounds for these issues.	9.8	More Details
CVE-2024-39250	EfroTech Timetrax v8.3 was discovered to contain an unauthenticated SQL injection vulnerability via the q parameter in the search web interface.	9.8	More Details
CVE-2024-38944	An issue in Intelight X-1L Traffic controller Maxtime v.1.9.6 allows a remote attacker to execute arbitrary code via the /cgi-bin/generateForm.cgi?formID=142 component.	9.8	More Details
CVE-2024-28698	Directory Traversal vulnerability in Marimer LLC CSLA .Net before 8.0 allows a remote attacker to execute arbitrary code via a crafted script to the MobileFormatter component.	9.8	More Details
CVE-2024-20401	A vulnerability in the content scanning and message filtering features of Cisco Secure Email Gateway could allow an unauthenticated, remote attacker to overwrite arbitrary files on the underlying operating system. This vulnerability is due to improper handling of email attachments when file analysis and content filters are enabled. An attacker could exploit this vulnerability by sending an email that contains a crafted attachment through an affected device. A successful exploit could allow the attacker to replace any file on the underlying file system. The attacker could then perform any of the following actions: add users with root privileges, modify the device configuration, execute arbitrary code, or cause a permanent denial of service (DoS) condition on the affected device. Note: Manual intervention is required to recover from the DoS condition. Customers are advised to contact the Cisco Technical Assistance Center (TAC) to help recover a device in this condition.	9.8	More Details
CVE-2024-41184	In the vrrp_ipsets_handler handler (fglobal_parser.c) of keepalived through 2.3.1, an integer overflow can occur. NOTE: this CVE Record might not be worthwhile because an empty ipset name must be configured by the user.	9.8	More Details
CVE-2024-6164	The Filter & Grids WordPress plugin before 2.8.33 is vulnerable to Local File Inclusion via the post_layout parameter. This makes it possible for an unauthenticated attacker to include and execute PHP files on the server, allowing the execution of any PHP code in those files.	9.8	More Details
CVE-2024-26020	An arbitrary script execution vulnerability exists in the MPV functionality of Ankitects Anki 24.04. A specially crafted flashcard can lead to a arbitrary code execution. An attacker can send malicious flashcard to trigger this vulnerability.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38164	An improper access control vulnerability in GroupMe allows an a unauthenticated attacker to elevate privileges over a network by convincing a user to click on a malicious link.	9.6	More Details
CVE-2024-41603	Spina CMS v2.18.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via the URI /admin/layout.	9.6	More Details
CVE-2024-5619	Authorization Bypass Through User-Controlled Key vulnerability in PruvaSoft Informatics Apinizer Management Console allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Apinizer Management Console: before 2024.05.1.	9.6	More Details
CVE-2024-28074	It was discovered that a previous vulnerability was not completely fixed with SolarWinds Access Rights Manager. While some controls were implemented the researcher was able to bypass these and use a different method to exploit the vulnerability.	9.6	More Details
CVE-2024-23475	The SolarWinds Access Rights Manager was susceptible to a Directory Traversal and Information Disclosure Vulnerability. This vulnerability allows an unauthenticated user to perform arbitrary file deletion and leak sensitive information.	9.6	More Details
CVE-2024-23472	SolarWinds Access Rights Manager (ARM) is susceptible to Directory Traversal vulnerability. This vulnerability allows an authenticated user to arbitrary read and delete files in ARM.	9.6	More Details
CVE-2024-23471	The SolarWinds Access Rights Manager was found to be susceptible to a Remote Code Execution Vulnerability. If exploited, this vulnerability allows an authenticated user to abuse a SolarWinds service resulting in remote code execution.	9.6	More Details
CVE-2024-23470	The SolarWinds Access Rights Manager was found to be susceptible to a pre-authentication remote code execution vulnerability. If exploited, this vulnerability allows an unauthenticated user to run commands and executables.	9.6	More Details
CVE-2024-23469	SolarWinds Access Rights Manager (ARM) is susceptible to a Remote Code Execution vulnerability. If exploited, this vulnerability allows an unauthenticated user to perform the actions with SYSTEM privileges.	9.6	More Details
CVE-2024-23467	The SolarWinds Access Rights Manager was susceptible to a Directory Traversal and Information Disclosure Vulnerability. This vulnerability allows an unauthenticated user to perform remote code execution.	9.6	More Details
CVE-2024-23466	SolarWinds Access Rights Manager (ARM) is susceptible to a Directory Traversal Remote Code Execution vulnerability. If exploited, this vulnerability allows an unauthenticated user to perform the actions with SYSTEM privileges.	9.6	More Details
CVE-2024-38773	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Adrian Tobey FormLift for Infusionsoft Web Forms allows Blind SQL Injection.This issue affects FormLift for Infusionsoft Web Forms: from n/a through 7.5.17.	9.3	More Details
CVE-2024-31070	Initialization of a resource with an insecure default vulnerability in FutureNet NXR series, VXR series and WXR series provided by Century Systems Co., Ltd. allows a remote unauthenticated attacker to access telnet service unlimitedly.	9.1	More Details
CVE-2024-29070	On versions before 2.1.4, session is not invalidated after logout. When the user logged in successfully, the Backend service returns "Authorization" as the front-end authentication credential. "Authorization" can still initiate requests and access data even after logout. Mitigation: all users should upgrade to 2.1.4	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29736	A SSRF vulnerability in WADL service description in versions of Apache CXF before 4.0.5, 3.6.4 and 3.5.9 allows an attacker to perform SSRF style attacks on REST webservices. The attack only applies if a custom stylesheet parameter is configured.	9.1	More Details
CVE-2024-6834	A vulnerability in APIML Spring Cloud Gateway which leverages user privileges by unexpected signing proxied request by Zowe's client certificate. This allows access to a user to the endpoints requiring an internal client certificate without any credentials. It could lead to managing components in there and allow an attacker to handle the whole communication including user credentials.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-25638	dnsjava is an implementation of DNS in Java. Records in DNS replies are not checked for their relevance to the query, allowing an attacker to respond with RRs from different zones. This vulnerability is fixed in 3.6.0.	8.9	More Details
CVE-2024-6338	The FV Flowplayer Video Player plugin for WordPress is vulnerable to time-based SQL Injection via the ‘exclude’ parameter in all versions up to, and including, 7.5.46.7212 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 Subscriber-level access and above, 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-2024-6913	Execution with unnecessary privileges in PerkinElmer ProcessPlus allows an attacker to spawn a remote shell on the windows system.This issue affects ProcessPlus: through 1.11.6507.0.	8.8	More Details
CVE-2024-20435	A vulnerability in the CLI of Cisco AsyncOS for Secure Web Appliance could allow an authenticated, local attacker to execute arbitrary commands and elevate privileges to root. This vulnerability is due to insufficient validation of user-supplied input for the CLI. An attacker could exploit this vulnerability by authenticating to the system and executing a crafted command on the affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root. To successfully exploit this vulnerability, an attacker would need at least guest credentials.	8.8	More Details
CVE-2024-5471	Zohocorp ManageEngine DDI Central versions 4001 and prior were vulnerable to agent takeover vulnerability due to the hard-coded sensitive keys.	8.8	More Details
CVE-2024-41320	TOTOLINK A6000R V1.0.1-B20201211.2000 was discovered to contain a command injection vulnerability via the ifname parameter in the get_apcli_conn_info function.	8.8	More Details
CVE-2024-31411	Unrestricted Upload of File with dangerous type vulnerability in Apache StreamPipes. Such a dangerous type might be an executable file that may lead to a remote code execution (RCE). The unrestricted upload is only possible for authenticated and authorized users. This issue affects Apache StreamPipes: through 0.93.0. Users are recommended to upgrade to version 0.95.0, which fixes the issue.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36475	FutureNet NXR series, VXR series and WXR series provided by Century Systems Co., Ltd. contain an active debug code vulnerability. If a user who knows how to use the debug function logs in to the product, the debug function may be used and an arbitrary OS command may be executed.	8.8	More Details
CVE-2024-40119	Nepstech Wifi Router xpon (terminal) model NTPL-Xpon1GFEVN v.1.0 Firmware V2.0.1 contains a Cross-Site Request Forgery (CSRF) vulnerability in the password change function, which allows remote attackers to change the admin password without the user's consent, leading to a potential account takeover.	8.8	More Details
CVE-2024-6497	The SEO Plugin by Squirrly SEO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘url’ parameter in all versions up to, and including, 12.3.19 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.	8.8	More Details
CVE-2024-5726	The Timeline Event History plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.1 via deserialization of untrusted input 'timelines-data' parameter. 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 software. 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-2024-29014	Vulnerability in SonicWall SMA100 NetExtender Windows (32 and 64-bit) client 10.2.339 and earlier versions allows an attacker to arbitrary code execution when processing an EPC Client update.	8.8	More Details
CVE-2024-39877	Apache Airflow 2.4.0, and versions before 2.9.3, has a vulnerability that allows authenticated DAG authors to craft a doc_md parameter in a way that could execute arbitrary code in the scheduler context, which should be forbidden according to the Airflow Security model. Users should upgrade to version 2.9.3 or later which has removed the vulnerability.	8.8	More Details
CVE-2024-3242	The Brizy – Page Builder plugin for WordPress is vulnerable to arbitrary file uploads due to missing file extension validation in the validateImageContent function called via storeImages in all versions up to, and including, 2.4.43. This makes it possible for authenticated attackers, with contributor access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. Version 2.4.44 prevents the upload of files ending in .sh and .php. Version 2.4.45 fully patches the issue.	8.8	More Details
CVE-2024-29178	On versions before 2.1.4, a user could log in and perform a template injection attack resulting in Remote Code Execution on the server, The attacker must successfully log into the system to launch an attack, so this is a moderate-impact vulnerability. Mitigation: all users should upgrade to 2.1.4	8.8	More Details
CVE-2024-6660	The BookingPress – Appointment Booking Calendar Plugin and Online Scheduling Plugin plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the bookingpress_import_data_continue_process_func function in all versions up to, and including, 1.1.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary options on the WordPress site and upload arbitrary files. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6467	The BookingPress – Appointment Booking Calendar Plugin and Online Scheduling Plugin plugin for WordPress is vulnerable to Arbitrary File Read to Arbitrary File Creation in all versions up to, and including, 1.1.5 via the 'bookingpress_save_lite_wizard_settings_func' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create arbitrary files that contain the content of files on the server, allowing the execution of any PHP code in those files or the exposure of sensitive information.	8.8	More Details
CVE-2024-41121	Woodpecker is a simple yet powerful CI/CD engine with great extensibility. The server allow to create any user who can trigger a pipeline run malicious workflows: 1. Those workflows can either lead to a host takeover that runs the agent executing the workflow. 2. Or allow to extract the secrets who would be normally provided to the plugins who's entrypoint are overwritten. This issue has been addressed in release version 2.7.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2024-6244	The PZ Frontend Manager WordPress plugin before 1.0.6 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	8.8	More Details
CVE-2024-5973	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.3.24 does not prevent students from creating instructor accounts, which could be used to get access to functionalities they shouldn't have.	8.8	More Details
CVE-2024-6965	A vulnerability has been found in Tenda O3 1.0.0.10 and classified as critical. Affected by this vulnerability is the function fromVirtualSet. The manipulation of the argument ip/localPort/publicPort/app leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272119. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2020-11640	AdvaBuild uses a command queue to launch certain operations. An attacker who gains access to the command queue can use it to launch an attack by running any executable on the AdvaBuild node. The executables that can be run are not limited to AdvaBuild specific executables. Improper Privilege Management vulnerability in ABB Advant MOD 300 AdvaBuild.This issue affects Advant MOD 300 AdvaBuild: from 3.0 through 3.7 SP2.	8.8	More Details
CVE-2024-6964	A vulnerability, which was classified as critical, was found in Tenda O3 1.0.0.10. Affected is the function fromDhcpSetSer. The manipulation of the argument dhcpEn/startIP/endIP/preDNS/altDNS/mask/gateway leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-272118 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-6963	A vulnerability, which was classified as critical, has been found in Tenda O3 1.0.0.10. This issue affects the function formexeCommand. The manipulation of the argument cmdinput leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272117 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-6962	A vulnerability classified as critical was found in Tenda O3 1.0.0.10. This vulnerability affects the function formQosSet. The manipulation of the argument remark/ipRange/upSpeed/downSpeed/enable leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272116. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6714	An issue was discovered in provd before version 0.1.5 with a setuid binary, which allows a local attacker to escalate their privilege.	8.8	More Details
CVE-2024-23321	For RocketMQ versions 5.2.0 and below, under certain conditions, there is a risk of exposure of sensitive Information to an unauthorized actor even if RocketMQ is enabled with authentication and authorization functions. An attacker, possessing regular user privileges or listed in the IP whitelist, could potentially acquire the administrator's account and password through specific interfaces. Such an action would grant them full control over RocketMQ, provided they have access to the broker IP address list. To mitigate these security threats, it is strongly advised that users upgrade to version 5.3.0 or newer. Additionally, we recommend users to use RocketMQ ACL 2.0 instead of the original RocketMQ ACL when upgrading to version Apache RocketMQ 5.3.0.	8.8	More Details
CVE-2024-41281	Linksys WRT54G v4.21.5 has a stack overflow vulnerability in get_merge_mac function.	8.8	More Details
CVE-2024-41602	Cross Site Request Forgery vulnerability in Spina CMS v.2.18.0 and before allows a remote attacker to escalate privileges via a crafted URL	8.8	More Details
CVE-2024-40400	An arbitrary file upload vulnerability in the image upload function of Automad v2.0.0 allows attackers to execute arbitrary code via a crafted file.	8.8	More Details
CVE-2024-6420	The Hide My WP Ghost WordPress plugin before 5.2.02 does not prevent redirects to the login page via the auth_redirect WordPress function, allowing an unauthenticated visitor to access the hidden login page.	8.6	More Details
CVE-2023-7272	In Eclipse Parsson before 1.0.4 and 1.1.3, a document with a large depth of nested objects can allow an attacker to cause a Java stack overflow exception and denial of service. Eclipse Parsson allows processing (e.g. parse, generate, transform and query) JSON documents.	8.6	More Details
CVE-2024-38708	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in UkrSolution Barcode Scanner with Inventory & Order Manager allows SQL Injection.This issue affects Barcode Scanner with Inventory & Order Manager: from n/a through 1.6.1.	8.5	More Details
CVE-2024-38755	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Designinvento DirectoryPress allows SQL Injection.This issue affects DirectoryPress: from n/a through 3.6.10.	8.5	More Details
CVE-2024-34329	Insecure permissions in Entrust Datacard XPS Card Printer Driver 8.4 and earlier allows unauthenticated attackers to execute arbitrary code as SYSTEM via a crafted DLL payload.	8.4	More Details
CVE-2024-41668	The cBioPortal for Cancer Genomics provides visualization, analysis, and download of large-scale cancer genomics data sets. When running a publicly exposed proxy endpoint without authentication, cBioPortal could allow someone to perform a Server Side Request Forgery (SSRF) attack. Logged in users could do the same on private instances. A fix has been released in version 6.0.12. As a workaround, one might be able to disable `/proxy` endpoint entirely via, for example, nginx.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23465	The SolarWinds Access Rights Manager was found to be susceptible to an authentication bypass vulnerability. This vulnerability allows an unauthenticated user to gain domain admin access within the Active Directory environment.	8.3	More Details
CVE-2024-39906	A command injection vulnerability was found in the IndieAuth functionality of the Ruby on Rails based Haven blog web application. The affected functionality requires authentication, but an attacker can craft a link that they can pass to a logged in administrator of the blog software. This leads to the immediate execution of the provided commands when the link is accessed by the authenticated administrator. This issue may lead to Remote Code Execution (RCE) and has been addressed by commit `c52f07c`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.3	More Details
CVE-2024-35199	TorchServe is a flexible and easy-to-use tool for serving and scaling PyTorch models in production. In affected versions the two gRPC ports 7070 and 7071, are not bound to localhost by default, so when TorchServe is launched, these two interfaces are bound to all interfaces. Customers using PyTorch inference Deep Learning Containers (DLC) through Amazon SageMaker and EKS are not affected. This issue in TorchServe has been fixed in PR #3083. TorchServe release 0.11.0 includes the fix to address this vulnerability. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.2	More Details
CVE-2023-40159	A validated user not explicitly authorized to have access to certain sensitive information could access Philips Vue PACS on the same network to expose that information.	8.2	More Details
CVE-2024-21527	Versions of the package github.com/gotenberg/gotenberg/v8/pkg/gotenberg before 8.1.0; versions of the package github.com/gotenberg/gotenberg/v8/pkg/modules/chromium before 8.1.0; versions of the package github.com/gotenberg/gotenberg/v8/pkg/modules/webhook before 8.1.0 are vulnerable to Server-side Request Forgery (SSRF) via the /convert/html endpoint when a request is made to a file via localhost, such as <iframe src="\\localhost/etc/passwd">. By exploiting this vulnerability, an attacker can achieve local file inclusion, allowing of sensitive files read on the host system. Workaround An alternative is using either or both --chromium-deny-list and --chromium-allow-list flags.	8.2	More Details
CVE-2024-40348	An issue in the component /api/swaggerui/static of Bazaar v1.4.3 allows unauthenticated attackers to execute a directory traversal.	8.2	More Details
CVE-2024-41107	The CloudStack SAML authentication (disabled by default) does not enforce signature check. In CloudStack environments where SAML authentication is enabled, an attacker that initiates CloudStack SAML single sign-on authentication can bypass SAML authentication by submitting a spoofed SAML response with no signature and known or guessed username and other user details of a SAML-enabled CloudStack user-account. In such environments, this can result in a complete compromise of the resources owned and/or accessible by a SAML enabled user-account. Affected users are recommended to disable the SAML authentication plugin by setting the "saml2.enabled" global setting to "false", or upgrade to version 4.18.2.2, 4.19.1.0 or later, which addresses this issue.	8.1	More Details
CVE-2024-38176	An improper restriction of excessive authentication attempts in GroupMe allows a unauthenticated attacker to elevate privileges over a network.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38447	NATO NCI ANET 3.4.1 allows Insecure Direct Object Reference via a modified ID field in a request for a private draft report (that belongs to an arbitrary user).	8.1	More Details
CVE-2024-6885	The MaxiBlocks: 2200+ Patterns, 190 Pages, 14.2K Icons & 100 Styles plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the maxi_remove_custom_image_size and maxi_add_custom_image_size functions in all versions up to, and including, 1.9.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	8.1	More Details
CVE-2024-40642	The netty incubator codec.bhttp is a java language binary http parser. In affected versions the `BinaryHttpParser` class does not properly validate input values thus giving attackers almost complete control over the HTTP requests constructed from the parsed output. Attackers can abuse several issues individually to perform various injection attacks including HTTP request smuggling, desync attacks, HTTP header injections, request queue poisoning, caching attacks and Server Side Request Forgery (SSRF). Attacker could also combine several issues to create well-formed messages for other text-based protocols which may result in attacks beyond the HTTP protocol. The BinaryHttpParser class implements the readRequestHead method which performs most of the relevant parsing of the received request. The data structure prefixes values with a variable length integer value. The parsing code below first gets the lengths of the values from the prefixed variable length integer. After it has all of the lengths and calculates all of the indices, the parser casts the applicable slices of the ByteBuf to String. Finally, it passes these values into a new `DefaultBinaryHttpRequest` object where no further parsing or validation occurs. Method is partially validated while other values are not validated at all. Software that relies on netty to apply input validation for binary HTTP data may be vulnerable to various injection and protocol based attacks. This issue has been addressed in version 0.0.13.Final. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.1	More Details
CVE-2024-39963	AX3000 Dual-Band Gigabit Wi-Fi 6 Router AX9 V22.03.01.46 and AX3000 Dual-Band Gigabit Wi-Fi 6 Router AX12 V1.0 V22.03.01.46 were discovered to contain an authenticated remote command execution (RCE) vulnerability via the macFilterType parameter at /goform/setMacFilterCfg.	8.0	More Details
CVE-2024-41317	TOTOLINK A6000R V1.0.1-B20201211.2000 was discovered to contain a command injection vulnerability via the ifname parameter in the apcli_do_enr_pbc_wps function.	8.0	More Details
CVE-2024-4080	A memory corruption issue due to an improper length check in LabVIEW tdcore.dll may disclose information or result in arbitrary code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	7.8	More Details
CVE-2024-6121	An out-of-date version of Redis shipped with NI SystemLink Server is susceptible to multiple vulnerabilities, including CVE-2022-24834. This affects NI SystemLink Server 2024 Q1 and prior versions. It also affects NI FlexLogger 2023 Q2 and prior versions which installed this shared service.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11639	An attacker could exploit the vulnerability by injecting garbage data or specially crafted data. Depending on the data injected each process might be affected differently. The process could crash or cause communication issues on the affected node, effectively causing a denial-of-service attack. The attacker could tamper with the data transmitted, causing the product to store wrong information or act on wrong data or display wrong information. This issue affects Advant MOD 300 AdvaBuild: from 3.0 through 3.7 SP2. For an attack to be successful, the attacker must have local access to a node in the system and be able to start a specially crafted application that disrupts the communication. An attacker who successfully exploited the vulnerability would be able to manipulate the data in such way as allowing reads and writes to the controllers or cause Windows processes in 800xA for MOD 300 and AdvaBuild to crash.	7.8	More Details
CVE-2024-4081	A memory corruption issue due to an improper length check in NI LabVIEW may disclose information or result in arbitrary code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects NI LabVIEW 2024 Q1 and prior versions.	7.8	More Details
CVE-2024-37391	ProtonVPN before 3.2.10 on Windows mishandles the drive installer path, which should use this: "" + ExpandConstant('{autopf}\Proton\Drive') + "" in Setup/setup.iss.	7.8	More Details
CVE-2024-6791	A directory path traversal vulnerability exists when loading a vsmodel file in NI VeriStand that may result in remote code execution. Successful exploitation requires an attacker to get a user to open a specially crafted .vsmodel file. This vulnerability affects VeriStand 2024 Q2 and prior versions.	7.8	More Details
CVE-2024-6675	A deserialization of untrusted data vulnerability exists in NI VeriStand 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 VeriStand 2024 Q2 and prior versions.	7.8	More Details
CVE-2024-5602	A stack-based buffer overflow vulnerability due to a missing bounds check in the NI I/O Trace Tool may result in arbitrary code execution. Successful exploitation requires an attacker to provide a user with a specially crafted nitrace file. The NI I/O Trace tool is installed as part of the NI System Configuration utilities included with many NI software products. Refer to the NI Security Advisory for identifying the version of NI IO Trace.exe installed. The NI I/O Trace tool was also previously released as NI Spy.	7.8	More Details
CVE-2024-4079	An out of bounds read due to a missing bounds check in LabVIEW may disclose information or result in arbitrary code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	7.8	More Details
CVE-2024-40724	Heap-based buffer overflow vulnerability in Assimp versions prior to 5.4.2 allows a local attacker to execute arbitrary code by inputting a specially crafted file into the product.	7.8	More Details
CVE-2024-41011	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: don't allow mapping the MMIO HDP page with large pages We don't get the right offset in that case. The GPU has an unused 4K area of the register BAR space into which you can remap registers. We remap the HDP flush registers into this space to allow userspace (CPU or GPU) to flush the HDP when it updates VRAM. However, on systems with >4K pages, we end up exposing PAGE_SIZE of MMIO space.	7.8	More Details
CVE-2024-6717	HashiCorp Nomad and Nomad Enterprise 1.6.12 up to 1.7.9, and 1.8.1 archive unpacking during migration is vulnerable to path escaping of the allocation directory. This vulnerability, CVE-2024-6717, is fixed in Nomad 1.6.13, 1.7.10, and 1.8.2.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38692	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Spiffy Plugins Spiffy Calendar allows SQL Injection.This issue affects Spiffy Calendar: from n/a through 4.9.11.	7.6	More Details
CVE-2024-23474	The SolarWinds Access Rights Manager was found to be susceptible to an Arbitrary File Deletion and Information Disclosure vulnerability.	7.6	More Details
CVE-2024-23468	The SolarWinds Access Rights Manager was susceptible to a Directory Traversal and Information Disclosure Vulnerability. This vulnerability allows an unauthenticated user to perform arbitrary file deletion and leak sensitive information.	7.6	More Details
CVE-2020-24102	Directory Traversal vulnerability in Punkbuster pbsv.d64 2.351, allows remote attackers to execute arbitrary code.	7.6	More Details
CVE-2024-38788	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Bởi Admin 2020 UiPress lite allows SQL Injection.This issue affects UiPress lite: from n/a through 3.4.06.	7.6	More Details
CVE-2024-28992	The SolarWinds Access Rights Manager was susceptible to a Directory Traversal and Information Disclosure Vulnerability. This vulnerability allows an unauthenticated user to perform arbitrary file deletion and leak sensitive information.	7.6	More Details
CVE-2024-28993	The SolarWinds Access Rights Manager was susceptible to a Directory Traversal and Information Disclosure Vulnerability. This vulnerability allows an unauthenticated user to perform arbitrary file deletion and leak sensitive information.	7.6	More Details
CVE-2024-40764	Heap-based buffer overflow vulnerability in the SonicOS IPSec VPN allows an unauthenticated remote attacker to cause Denial of Service (DoS).	7.5	More Details
CVE-2024-4076	Client queries that trigger serving stale data and that also require lookups in local authoritative zone data may result in an assertion failure. This issue affects BIND 9 versions 9.16.13 through 9.16.50, 9.18.0 through 9.18.27, 9.19.0 through 9.19.24, 9.11.33-S1 through 9.11.37-S1, 9.16.13-S1 through 9.16.50-S1, and 9.18.11-S1 through 9.18.27-S1.	7.5	More Details
CVE-2024-41655	TF2 Item Format helps users format TF2 items to the community standards. Versions of `tf2-item-format` since at least `4.2.6` and prior to `5.9.14` are vulnerable to a Regular Expression Denial of Service (ReDoS) attack when parsing crafted user input. This vulnerability can be exploited by an attacker to perform DoS attacks on any service that uses any `tf2-item-format` to parse user input. Version `5.9.14` contains a fix for the issue.	7.5	More Details
CVE-2024-41492	A stack overflow in Tenda AX1806 v1.0.0.1 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-41601	Insecure Permissions vulnerability in lin-CMS v.0.2.0 and before allows a remote attacker to obtain sensitive information via the login method in the UserController.java component.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31143	An optional feature of PCI MSI called "Multiple Message" allows a device to use multiple consecutive interrupt vectors. Unlike for MSI-X, the setting up of these consecutive vectors needs to happen all in one go. In this handling an error path could be taken in different situations, with or without a particular lock held. This error path wrongly releases the lock even when it is not currently held.	7.5	More Details
CVE-2024-6960	The H2O machine learning platform uses "Iced" classes as the primary means of moving Java Objects around the cluster. The Iced format supports inclusion of serialized Java objects. When a model is deserialized, any class is allowed to be deserialized (no class whitelist). An attacker can construct a crafted Iced model that uses Java gadgets and leads to arbitrary code execution when imported to the H2O platform.	7.5	More Details
CVE-2024-40060	go-chart v2.1.1 was discovered to contain an infinite loop via the drawCanvas() function.	7.5	More Details
CVE-2024-41600	Insecure Permissions vulnerability in lin-CMS Springboot v.0.2.1 and before allows a remote attacker to obtain sensitive information via the login method in the UserController.java component.	7.5	More Details
CVE-2024-1975	If a server hosts a zone containing a "KEY" Resource Record, or a resolver DNSSEC-validates a "KEY" Resource Record from a DNSSEC-signed domain in cache, a client can exhaust resolver CPU resources by sending a stream of SIG(0) signed requests. This issue affects BIND 9 versions 9.0.0 through 9.11.37, 9.16.0 through 9.16.50, 9.18.0 through 9.18.27, 9.19.0 through 9.19.24, 9.9.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.49-S1, and 9.18.11-S1 through 9.18.27-S1.	7.5	More Details
CVE-2024-40898	SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue.	7.5	More Details
CVE-2024-41122	Woodpecker is a simple yet powerful CI/CD engine with great extensibility. The server allow to create any user who can trigger a pipeline run malicious workflows: 1. Those workflows can either lead to a host takeover that runs the agent executing the workflow. 2. Or allow to extract the secrets who would be normally provided to the plugins who's entrypoint are overwritten. This issue has been addressed in release version 2.7.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2024-0760	A malicious client can send many DNS messages over TCP, potentially causing the server to become unstable while the attack is in progress. The server may recover after the attack ceases. Use of ACLs will not mitigate the attack. This issue affects BIND 9 versions 9.18.1 through 9.18.27, 9.19.0 through 9.19.24, and 9.18.11-S1 through 9.18.27-S1.	7.5	More Details
CVE-2024-1737	Resolver caches and authoritative zone databases that hold significant numbers of RRs for the same hostname (of any RTYPE) can suffer from degraded performance as content is being added or updated, and also when handling client queries for this name. This issue affects BIND 9 versions 9.11.0 through 9.11.37, 9.16.0 through 9.16.50, 9.18.0 through 9.18.27, 9.19.0 through 9.19.24, 9.11.4-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.50-S1, and 9.18.11-S1 through 9.18.27-S1.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41178	Exposure of temporary credentials in logs in Apache Arrow Rust Object Store (`object_store` crate), version 0.10.1 and earlier on all platforms using AWS WebIdentityTokens. On certain error conditions, the logs may contain the OIDC token passed to AssumeRoleWithWebIdentity https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithWebIdentity.html . This allows someone with access to the logs to impersonate that identity, including performing their own calls to AssumeRoleWithWebIdentity, until the OIDC token expires. Typically OIDC tokens are valid for up to an hour, although this will vary depending on the issuer. Users are recommended to use a different AWS authentication mechanism, disable logging or upgrade to version 0.10.2, which fixes this issue. Details: When using AWS WebIdentityTokens with the object_store crate, in the event of a failure and automatic retry, the underlying reqwest error, including the full URL with the credentials, potentially in the parameters, is written to the logs. Thanks to Paul Hatcherian for reporting this vulnerability	7.5	More Details
CVE-2023-7269	The ArtPlacer Widget WordPress plugin before 2.21.2 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	7.5	More Details
CVE-2024-6911	Files on the Windows system are accessible without authentication to external parties due to a local file inclusion in PerkinElmer ProcessPlus.This issue affects ProcessPlus: through 1.11.6507.0.	7.5	More Details
CVE-2024-41172	In versions of Apache CXF before 3.6.4 and 4.0.5 (3.5.x and lower versions are not impacted), a CXF HTTP client conduit may prevent HTTPClient instances from being garbage collected and it is possible that memory consumption will continue to increase, eventually causing the application to run out of memory	7.5	More Details
CVE-2024-6805	The NI VeriStand Gateway is missing authorization checks when an actor attempts to access File Transfer resources. These missing checks may result in information disclosure or remote code execution. This affects NI VeriStand 2024 Q2 and prior versions.	7.5	More Details
CVE-2024-20323	A vulnerability in Cisco Intelligent Node (iNode) Software could allow an unauthenticated, remote attacker to hijack the TLS connection between Cisco iNode Manager and associated intelligent nodes and send arbitrary traffic to an affected device. This vulnerability is due to the presence of hard-coded cryptographic material. An attacker in a man-in-the-middle position between Cisco iNode Manager and associated deployed nodes could exploit this vulnerability by using the static cryptographic key to generate a trusted certificate and impersonate an affected device. A successful exploit could allow the attacker to read data that is meant for a legitimate device, modify the startup configuration of an associated node, and, consequently, cause a denial of service (DoS) condition for downstream devices that are connected to the affected node.	7.5	More Details
CVE-2024-40634	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. This report details a security vulnerability in Argo CD, where an unauthenticated attacker can send a specially crafted large JSON payload to the /api/webhook endpoint, causing excessive memory allocation that leads to service disruption by triggering an Out Of Memory (OOM) kill. The issue poses a high risk to the availability of Argo CD deployments. This vulnerability is fixed in 2.11.6, 2.10.15, and 2.9.20.	7.5	More Details
CVE-2024-40051	IP Guard v4.81.0307.0 was discovered to contain an arbitrary file read vulnerability via the file name parameter.	7.5	More Details
CVE-2024-41131	ImageSharp is a 2D graphics API. An Out-of-bounds Write vulnerability has been found in the ImageSharp gif decoder, allowing attackers to cause a crash using a specially crafted gif. This can potentially lead to denial of service. All users are advised to upgrade to v3.1.5 or v2.1.9.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32007	An improper input validation of the p2c parameter in the Apache CXF JOSE code before 4.0.5, 3.6.4 and 3.5.9 allows an attacker to perform a denial of service attack by specifying a large value for this parameter in a token.	7.5	More Details
CVE-2024-40641	Nuclei is a fast and customizable vulnerability scanner based on simple YAML based DSL. In affected versions it a way to execute code template without -code option and signature has been discovered. Some web applications inherit from Nuclei and allow users to edit and execute workflow files. In this case, users can execute arbitrary commands. (Although, as far as I know, most web applications use -t to execute). This issue has been addressed in version 3.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.4	More Details
CVE-2024-41827	In JetBrains TeamCity before 2024.07 access tokens could continue working after deletion or expiration	7.4	More Details
CVE-2024-32484	An reflected XSS vulnerability exists in the handling of invalid paths in the Flask server in Ankitects Anki 24.04. A specially crafted flashcard can lead to JavaScript code execution and result in an arbitrary file read. An attacker can share a malicious flashcard to trigger this vulnerability.	7.4	More Details
CVE-2024-6966	A vulnerability was found in itsourcecode Online Blood Bank Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file login.php of the component Login. The manipulation of the argument user/pass 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-272120.	7.3	More Details
CVE-2024-6637	The WooCommerce - Social Login plugin for WordPress is vulnerable to unauthenticated privilege escalation in all versions up to, and including, 2.7.3. This is due to a lack of brute force controls on a weak one-time password. This makes it possible for unauthenticated attackers to brute force the one-time password for any user, except an Administrator, if they know the email of user.	7.3	More Details
CVE-2024-6808	A vulnerability was found in itsourcecode Simple Task List 1.0. It has been classified as critical. This affects the function insertUserRecord of the file signUp.php. The manipulation of the argument username 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-271707.	7.3	More Details
CVE-2024-6957	A vulnerability classified as critical has been found in itsourcecode University Management System 1.0. This affects an unknown part of the file functions.php of the component Login. The manipulation of the argument username 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-272079.	7.3	More Details
CVE-2024-6635	The WooCommerce - Social Login plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.7.3. This is due to insufficient controls in the 'woo_slg_login_email' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, excluding an administrator, if they know the email of user.	7.3	More Details
CVE-2024-6898	A vulnerability was found in SourceCodester Record Management System 1.0. It has been classified as critical. This affects an unknown part of the file index.php. The manipulation of the argument UserName 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-271923.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41111	Sliver is an open source cross-platform adversary emulation/red team framework, it can be used by organizations of all sizes to perform security testing. Sliver version 1.6.0 (prerelease) is vulnerable to RCE on the teamserver by a low-privileged "operator" user. The RCE is as the system root user. The exploit is pretty fun as we make the Sliver server pwn itself. As described in a past issue (#65), "there is a clear security boundary between the operator and server, an operator should not inherently be able to run commands or code on the server." An operator who exploited this vulnerability would be able to view all console logs, kick all other operators, view and modify files stored on the server, and ultimately delete the server. This issue has not yet be addressed but is expected to be resolved before the full release of version 1.6.0. Users of the 1.6.0 prerelease should avoid using Silver in production.	7.2	More Details
CVE-2024-6828	The Redux Framework plugin for WordPress is vulnerable to unauthenticated JSON file uploads due to missing authorization and capability checks on the Redux_Color_Scheme_Import function in versions 4.4.12 to 4.4.17. This makes it possible for unauthenticated attackers to upload JSON files, which can be used to conduct stored cross-site scripting attacks and, in some rare cases, when the wp_filesystem fails to initialize - to Remote Code Execution.	7.2	More Details
CVE-2024-38728	Server-Side Request Forgery (SSRF) vulnerability in Seraphinite Solutions Seraphinite Post .DOCX Source.This issue affects Seraphinite Post .DOCX Source: from n/a through 2.16.9.	7.2	More Details
CVE-2024-37942	Server-Side Request Forgery (SSRF) vulnerability in Berqier Ltd BerqWP.This issue affects BerqWP: from n/a through 1.7.5.	7.2	More Details
CVE-2024-37245	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Vsourz Digital All In One Redirection allows Reflected XSS.This issue affects All In One Redirection: from n/a through 2.2.0.	7.1	More Details
CVE-2024-37509	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Maksekeskus AS MakeCommerce for WooCommerce allows Reflected XSS.This issue affects MakeCommerce for WooCommerce: from n/a through 3.5.1.	7.1	More Details
CVE-2024-38781	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ArtistScope CopySafe Web Protection allows Reflected XSS.This issue affects CopySafe Web Protection: from n/a through 3.15.	7.1	More Details
CVE-2024-37559	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Echenley Counterpoint allows Reflected XSS.This issue affects Counterpoint: from n/a through 1.8.1.	7.1	More Details
CVE-2024-38711	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Yannick Lefebvre Link Library allows Reflected XSS.This issue affects Link Library: from n/a through 7.7.1.	7.1	More Details
CVE-2024-37920	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Repute InfoSystems ARForms Form Builder allows Reflected XSS.This issue affects ARForms Form Builder: from n/a through 1.6.7.	7.1	More Details
CVE-2024-37953	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MBE Worldwide S.P.A. MBE eShip allows Reflected XSS.This issue affects MBE eShip: from n/a through 2.1.2.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38696	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Zoho CRM Zoho CRM Lead Magnet allows Reflected XSS.This issue affects Zoho CRM Lead Magnet: from n/a through 1.7.8.8.	7.1	More Details
CVE-2024-38694	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Moloni allows Reflected XSS.This issue affects Moloni: from n/a through 4.7.4.	7.1	More Details
CVE-2024-37954	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in marcelotorres Simple Responsive Slider allows Reflected XSS.This issue affects Simple Responsive Slider: from n/a through 0.2.2.5.	7.1	More Details
CVE-2024-38683	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in iThemelandCo WooCommerce Report allows Reflected XSS.This issue affects WooCommerce Report: from n/a through 1.4.5.	7.1	More Details
CVE-2024-38680	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Appmaker Appmaker – Convert WooCommerce to Android & iOS Native Mobile Apps allows Reflected XSS.This issue affects Appmaker – Convert WooCommerce to Android & iOS Native Mobile Apps: from n/a through 1.36.12.	7.1	More Details
CVE-2024-37485	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Vinny Alves (UseStrict Consulting) bbPress Notify allows Reflected XSS.This issue affects bbPress Notify: from n/a through 2.18.3.	7.1	More Details
CVE-2024-37487	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in wpdirectorykit.Com WP Directory Kit allows Reflected XSS.This issue affects WP Directory Kit: from n/a through 1.3.5.	7.1	More Details
CVE-2024-38673	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Obtain Infotech Multisite Content Copier/Updater allows Reflected XSS.This issue affects Multisite Content Copier/Updater: from n/a through 1.5.0.	7.1	More Details
CVE-2024-38672	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in namithjawahar AdPush allows Reflected XSS.This issue affects AdPush: from n/a through 1.50.	7.1	More Details
CVE-2024-38669	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in a3rev Software WooCommerce Predictive Search allows Reflected XSS.This issue affects WooCommerce Predictive Search: from n/a through 6.0.1.	7.1	More Details
CVE-2024-37961	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in codoc.Jp allows Stored XSS.This issue affects codoc: from n/a through 0.9.51.12.	7.1	More Details
CVE-2024-37459	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PayPlus LTD PayPlus Payment Gateway allows Reflected XSS.This issue affects PayPlus Payment Gateway: from n/a through 6.6.8.	7.1	More Details
CVE-2024-37461	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Martin Gibson IdeaPush allows Stored XSS.This issue affects IdeaPush: from n/a through 8.65.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41656	Sentry is an error tracking and performance monitoring platform. Starting in version 10.0.0 and prior to version 24.7.1, an unsanitized payload sent by an Integration platform integration allows storing arbitrary HTML tags on the Sentry side with the subsequent rendering them on the Issues page. Self-hosted Sentry users may be impacted in case of untrustworthy Integration platform integrations sending external issues from their side to Sentry. A patch has been released in Sentry 24.7.1. For Sentry SaaS customers, no action is needed. This has been patched on July 23, and even prior to the fix, the exploitation was not possible due to the strict Content Security Policy deployed on sentry.io site. For self-hosted users, the maintainers of Sentry strongly recommend upgrading Sentry to the latest version. If it is not possible, one could enable CSP on one's self-hosted installation with `CSP_REPORT_ONLY = False` (enforcing mode). This will mitigate the risk of cross-site scripting.	7.1	More Details
CVE-2024-37433	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in EverPress Mailster allows Reflected XSS.This issue affects Mailster: from n/a through 4.0.9.	7.1	More Details
CVE-2024-37257	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Maciej Bis Permalink Manager Lite allows Reflected XSS.This issue affects Permalink Manager Lite: from n/a through 2.4.3.3.	7.1	More Details
CVE-2024-37432	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeGrill Esteem allows Stored XSS.This issue affects Esteem: from n/a through 1.5.0.	7.1	More Details
CVE-2024-37211	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ali2Woo Team Ali2Woo Lite allows Reflected XSS.This issue affects Ali2Woo Lite: from n/a through 3.3.5.	7.1	More Details
CVE-2024-37206	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Theme4Press Demo Awesome allows Reflected XSS.This issue affects Demo Awesome: from n/a through 1.0.1.	7.1	More Details
CVE-2024-37258	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Social Rocket allows Reflected XSS.This issue affects Social Rocket: from n/a through 1.3.3.	7.1	More Details
CVE-2024-37199	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kriesi.At Enfold allows Reflected XSS.This issue affects Enfold: from n/a through 5.6.9.	7.1	More Details
CVE-2024-37117	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Uncanny Owl Uncanny Automator Pro allows Reflected XSS.This issue affects Uncanny Automator Pro: from n/a through 5.3.	7.1	More Details
CVE-2024-40492	Cross Site Scripting vulnerability in Heartbeat Chat v.15.2.1 allows a remote attacker to execute arbitrary code via the setname function.	7.1	More Details
CVE-2023-50304	IBM Engineering Requirements Management DOORS Web Access 9.7.2.8 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 273335.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37097	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in UnitedThemes Shortcodes by United Themes allows Reflected XSS.This issue affects Shortcodes by United Themes: from n/a before 5.0.5.	7.1	More Details
CVE-2024-35656	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Elementor Elementor Pro allows Reflected XSS.This issue affects Elementor Pro: from n/a through 3.21.2.	7.1	More Details
CVE-2024-37436	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Uncanny Owl Uncanny Toolkit Pro for LearnDash allows Reflected XSS.This issue affects Uncanny Toolkit Pro for LearnDash: from n/a before 4.1.4.1.	7.1	More Details
CVE-2023-40704	Philips Vue PACS uses default credentials for potentially critical functionality.	7.1	More Details
CVE-2024-0981	Okta Browser Plugin versions 6.5.0 through 6.31.0 (Chrome/Edge/Firefox/Safari) are vulnerable to cross-site scripting. This issue occurs when the plugin prompts the user to save these credentials within Okta Personal. A fix was implemented to properly escape these fields, addressing the vulnerability. Importantly, if Okta Personal is not added to the plugin to enable multi-account view, the Workforce Identity Cloud plugin is not affected by this issue. The vulnerability is fixed in Okta Browser Plugin version 6.32.0 for Chrome/Edge/Safari/Firefox.	7.1	More Details
CVE-2024-37275	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NextScripts allows Reflected XSS.This issue affects NextScripts: from n/a through 4.4.6.	7.1	More Details
CVE-2024-37264	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Groundhogg Inc. Groundhogg allows Reflected XSS.This issue affects Groundhogg: from n/a through 3.4.2.3.	7.1	More Details
CVE-2024-37262	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in vCita.Com Online Booking & Scheduling Calendar for WordPress by vcita allows Reflected XSS.This issue affects Online Booking & Scheduling Calendar for WordPress by vcita: from n/a through 4.4.2.	7.1	More Details
CVE-2024-37261	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Lab WP-Lister Lite for Amazon allows Reflected XSS.This issue affects WP-Lister Lite for Amazon: from n/a through 2.6.16.	7.1	More Details
CVE-2024-37416	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in J.N. Breetvelt a.K.A. OpaJaap WP Photo Album Plus allows Reflected XSS.This issue affects WP Photo Album Plus: from n/a through 8.8.00.002.	7.1	More Details
CVE-2024-37259	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Extended The Ultimate WordPress Toolkit – WP Extended allows Reflected XSS.This issue affects The Ultimate WordPress Toolkit – WP Extended: from n/a through 2.4.7.	7.1	More Details
CVE-2024-37267	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in kaptinlin Striking allows Reflected XSS.This issue affects Striking: from n/a through 2.3.4.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41314	TOTOLINK A6000R V1.0.1-B20201211.2000 was discovered to contain a command injection vulnerability via the iface parameter in the vif_disable function.	6.8	More Details
CVE-2024-38302	Dell Data Lakehouse, version(s) 1.0.0.0, contain(s) a Missing Encryption of Sensitive Data vulnerability in the DDAE (Starburst). A low privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to Information disclosure.	6.8	More Details
CVE-2024-41315	TOTOLINK A6000R V1.0.1-B20201211.2000 was discovered to contain a command injection vulnerability via the ifname parameter in the apcli_do_enr_pin_wps function.	6.8	More Details
CVE-2024-40644	gitoxide An idiomatic, lean, fast & safe pure Rust implementation of Git. `gix-path` can be tricked into running another `git.exe` placed in an untrusted location by a limited user account on Windows systems. Windows permits limited user accounts without administrative privileges to create new directories in the root of the system drive. While `gix-path` first looks for `git` using a `PATH` search, in version 0.10.8 it also has a fallback strategy on Windows of checking two hard-coded paths intended to be the 64-bit and 32-bit Program Files directories. Existing functions, as well as the newly introduced `exe_invocation` function, were updated to make use of these alternative locations. This causes facilities in `gix_path::env` to directly execute `git.exe` in those locations, as well as to return its path or whatever configuration it reports to callers who rely on it. Although unusual setups where the system drive is not `C:`, or even where Program Files directories have non-default names, are technically possible, the main problem arises on a 32-bit Windows system. Such a system has no `C:\Program Files (x86)` directory. A limited user on a 32-bit Windows system can therefore create the `C:\Program Files (x86)` directory and populate it with arbitrary contents. Once a payload has been placed at the second of the two hard-coded paths in this way, other user accounts including administrators will execute it if they run an application that uses `gix-path` and do not have `git` in a `PATH` directory. (While having `git` found in a `PATH` search prevents exploitation, merely having it installed in the default location under the real `C:\Program Files` directory does not. This is because the first hard-coded path's `mingw64` component assumes a 64-bit installation.). Only Windows is affected. Exploitation is unlikely except on a 32-bit system. In particular, running a 32-bit build on a 64-bit system is not a risk factor. Furthermore, the attacker must have a user account on the system, though it may be a relatively unprivileged account. Such a user can perform privilege escalation and execute code as another user, though it may be difficult to do so reliably because the targeted user account must run an application or service that uses `gix-path` and must not have `git` in its `PATH`. The main exploitable configuration is one where Git for Windows has been installed but not added to `PATH`. This is one of the options in its installer, though not the default option. Alternatively, an affected program that sanitizes its `PATH` to remove seemingly nonessential directories could allow exploitation. But for the most part, if the target user has configured a `PATH` in which the real `git.exe` can be found, then this cannot be exploited. This issue has been addressed in release version 0.10.9 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	6.8	More Details
CVE-2024-37066	A command injection vulnerability exists in Wyze V4 Pro firmware versions before 4.50.4.9222, which allows attackers to execute arbitrary commands over Bluetooth as root during the camera setup process.	6.8	More Details
CVE-2024-37959	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Atlas Public Policy Power BI Embedded for WordPress allows Stored XSS.This issue affects Power BI Embedded for WordPress: from n/a through 1.1.7.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37244	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ninja Team Ninja Beaver Add-ons for Beaver Builder allows Stored XSS.This issue affects Ninja Beaver Add-ons for Beaver Builder: from n/a through 2.4.5.	6.5	More Details
CVE-2024-37229	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AuburnForest Blogmentor – Blog Layouts for Elementor allows Stored XSS.This issue affects Blogmentor – Blog Layouts for Elementor: from n/a through 1.5.	6.5	More Details
CVE-2024-37223	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Nicdark Restaurant Reservations allows Stored XSS.This issue affects Restaurant Reservations: from n/a through 2.0.	6.5	More Details
CVE-2024-38767	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BannerSky.Com BSK PDF Manager allows Stored XSS.This issue affects BSK PDF Manager: from n/a through 3.6.	6.5	More Details
CVE-2024-38434	Unitronics Vision PLC – CWE-676: Use of Potentially Dangerous Function may allow security feature bypass	6.5	More Details
CVE-2024-37221	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Michael Bester Kimili Flash Embed allows Stored XSS.This issue affects Kimili Flash Embed: from n/a through 2.5.3.	6.5	More Details
CVE-2024-37488	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in HelloAsso allows Stored XSS.This issue affects HelloAsso: from n/a through 1.1.9.	6.5	More Details
CVE-2024-37489	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in OceanWP Ocean Extra allows Stored XSS.This issue affects Ocean Extra: from n/a through 2.2.9.	6.5	More Details
CVE-2024-6542	Improper neutralization of livestatus command delimiters in mknotifyd in Checkmk <= 2.0.0p39, < 2.1.0p47, < 2.2.0p32 and < 2.3.0p11 allows arbitrary livestatus command execution.	6.5	More Details
CVE-2024-37918	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPCone.Com ConeBlog – WordPress Blog Widgets allows Stored XSS.This issue affects ConeBlog – WordPress Blog Widgets: from n/a through 1.4.8.	6.5	More Details
CVE-2024-39601	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V5.40), SICORE Base system (All versions < V1.4.0). Affected devices allow a remote authenticated user or an unauthenticated user with physical access to downgrade the firmware of the device. This could allow an attacker to downgrade the device to older versions with known vulnerabilities.	6.5	More Details
CVE-2024-37958	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Meks Meks Smart Author Widget allows Stored XSS.This issue affects Meks Smart Author Widget: from n/a through 1.1.4.	6.5	More Details
CVE-2024-37957	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in bradmax Bradmax Player allows Stored XSS.This issue affects Bradmax Player: from n/a through 1.1.27.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37955	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Zakaria Binsaifullah GutSlider – All in One Block Slider allows Stored XSS.This issue affects GutSlider – All in One Block Slider: from n/a through 2.7.3.	6.5	More Details
CVE-2024-37563	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in TOCHAT.BE allows Stored XSS.This issue affects TOCHAT.BE: from n/a through 1.3.0.	6.5	More Details
CVE-2024-4260	The Page Builder Gutenberg Blocks WordPress plugin before 3.1.12 does not prevent users from pinging arbitrary hosts via some of its shortcodes, which could allow high privilege users such as contributors to perform SSRF attacks.	6.5	More Details
CVE-2024-37495	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mediavine Create by Mediavine allows Stored XSS.This issue affects Create by Mediavine: from n/a through 1.9.7.	6.5	More Details
CVE-2024-37951	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Noor alam Magical Posts Display – Elementor & Gutenberg Posts Blocks allows Stored XSS.This issue affects Magical Posts Display – Elementor & Gutenberg Posts Blocks: from n/a through 1.2.38.	6.5	More Details
CVE-2024-37949	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CyberChimps Responsive Mobile allows Stored XSS.This issue affects Responsive Mobile: from n/a through 1.15.1.	6.5	More Details
CVE-2024-37948	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PootlePress Caxton – Create Pro page layouts in Gutenberg allows Stored XSS.This issue affects Caxton – Create Pro page layouts in Gutenberg: from n/a through 1.30.1.	6.5	More Details
CVE-2024-37944	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Travel Engine allows Stored XSS.This issue affects WP Travel Engine: from n/a through 5.9.1.	6.5	More Details
CVE-2024-39688	Bert-VITS2 is the VITS2 Backbone with multilingual bert. User input supplied to the data_dir variable is concatenated with other folders and used to open a new file in the generate_config function, which leads to a limited file write. The issue allows for writing /config/config.json file in arbitrary directory on the server. If a given directory path doesn't exist, the application will return an error, so this vulnerability could also be used to gain information about existing directories on the server. This affects fishaudio/Bert-VITS2 2.3 and earlier.	6.5	More Details
CVE-2024-37936	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in labibahmed Tabs For WPBakery Page Builder allows Stored XSS.This issue affects Tabs For WPBakery Page Builder: from n/a through 1.2.	6.5	More Details
CVE-2024-37922	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Leap13 Premium Addons for Elementor allows Stored XSS.This issue affects Premium Addons for Elementor: from n/a through 4.10.34.	6.5	More Details
CVE-2024-1575	The improper privilege management vulnerability in the Zyxel WBE660S firmware version 6.70(ACGG.3) and earlier versions could allow an authenticated user to escalate privileges and download the configuration files on a vulnerable device.	6.5	More Details
CVE-2024-37492	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Gutenberg Team Gutenberg allows Stored XSS.This issue affects Gutenberg: from n/a through 18.6.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37521	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in zwwooooo zBench allows Stored XSS.This issue affects zBench: from n/a through 1.4.2.	6.5	More Details
CVE-2024-37219	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PBN Hosting SL Page Builder Sandwich – Front-End Page Builder allows Stored XSS.This issue affects Page Builder Sandwich – Front-End Page Builder: from n/a through 5.1.0.	6.5	More Details
CVE-2024-37465	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Senol Sahin GPT3 AI Content Writer allows Stored XSS.This issue affects GPT3 AI Content Writer: from n/a through 1.8.66.	6.5	More Details
CVE-2024-37246	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jethin Gallery Slideshow allows Stored XSS.This issue affects Gallery Slideshow: from n/a through 1.4.1.	6.5	More Details
CVE-2024-37263	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeLooks Enter Addons enteraddons allows Stored XSS.This issue affects Enter Addons: from n/a through 2.1.6.	6.5	More Details
CVE-2024-37265	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Martin Gibson IdeaPush allows Stored XSS.This issue affects IdeaPush: from n/a through 8.60.	6.5	More Details
CVE-2024-37422	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Team Emilia Projects Progress Planner allows Stored XSS.This issue affects Progress Planner: from n/a through 0.9.2.	6.5	More Details
CVE-2024-37428	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themesgrove WidgetKit allows Stored XSS.This issue affects WidgetKit: from n/a through 2.5.0.	6.5	More Details
CVE-2024-37457	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ultimate Blocks Ultimate Blocks – Gutenberg Blocks Plugin allows Stored XSS.This issue affects Ultimate Blocks – Gutenberg Blocks Plugin: from n/a through 3.1.9.	6.5	More Details
CVE-2024-38782	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MapsMarker.Com e.U. Leaflet Maps Marker allows Stored XSS.This issue affects Leaflet Maps Marker: from n/a through 3.12.9.	6.5	More Details
CVE-2024-38750	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in digontoahsan Advanced post slider.This issue affects Advanced post slider: from n/a through 3.0.0.	6.5	More Details
CVE-2024-37445	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in bPlugins Html5 Audio Player allows Stored XSS.This issue affects Html5 Audio Player: from n/a through 2.2.23.	6.5	More Details
CVE-2024-37480	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Apollo13Themes Apollo13 Framework Extensions apollo13-framework-extensions allows Stored XSS.This issue affects Apollo13 Framework Extensions: from n/a through 1.9.3.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37466	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kraftplugins Mega Elements.This issue affects Mega Elements: from n/a through 1.2.2.	6.5	More Details
CVE-2024-33933	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brainstorm Force, Nikhil Chavan Elementor – Header, Footer & Blocks Template allows DOM-Based XSS.This issue affects Elementor – Header, Footer & Blocks Template: from n/a through 1.6.35.	6.5	More Details
CVE-2024-34457	On versions before 2.1.4, after a regular user successfully logs in, they can manually make a request using the authorization token to view everyone's user flink information, including executeSQL and config. Mitigation: all users should upgrade to 2.1.4	6.5	More Details
CVE-2024-37100	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mayur Somani, threeroutes media Elegant Themes Icons allows Stored XSS.This issue affects Elegant Themes Icons: from n/a through 1.3.	6.5	More Details
CVE-2024-37217	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ProWCPlugins Empty Cart Button for WooCommerce allows Stored XSS.This issue affects Empty Cart Button for WooCommerce: from n/a through 1.3.8.	6.5	More Details
CVE-2024-37101	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AF themes WP Post Author allows Stored XSS.This issue affects WP Post Author: from n/a through 3.6.7.	6.5	More Details
CVE-2024-37460	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SuperSaaS SuperSaaS – online appointment scheduling allows Stored XSS.This issue affects SuperSaaS – online appointment scheduling: from n/a through 2.1.9.	6.5	More Details
CVE-2024-37114	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Takashi Matsuyama My Favorites allows Stored XSS.This issue affects My Favorites: from n/a through 1.4.1.	6.5	More Details
CVE-2024-38786	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BurgerThemes CoziPress allows Stored XSS.This issue affects CoziPress: from n/a through 1.0.30.	6.5	More Details
CVE-2024-38785	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jegstudio Gutenverse allows Stored XSS.This issue affects Gutenverse: from n/a through 1.9.2.	6.5	More Details
CVE-2024-37116	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in sinatrateam Sinatra allows Stored XSS.This issue affects Sinatra: from n/a through 1.3.	6.5	More Details
CVE-2024-38435	Unitronics Vision PLC – CWE-703: Improper Check or Handling of Exceptional Conditions may allow denial of service	6.5	More Details
CVE-2024-37519	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Leap13 Premium Blocks – Gutenberg Blocks for WordPress allows Stored XSS.This issue affects Premium Blocks – Gutenberg Blocks for WordPress: from n/a through 2.1.27.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37514	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ArtistScope CopySafe Web Protection allows Stored XSS.This issue affects CopySafe Web Protection: from n/a through 3.14.	6.5	More Details
CVE-2024-37512	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Basix NEX-Forms – Ultimate Form Builder allows Stored XSS.This issue affects NEX-Forms – Ultimate Form Builder: from n/a through 8.5.10.	6.5	More Details
CVE-2024-37216	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Rami Yushuvaev Sketchfab Embed allows Stored XSS.This issue affects Sketchfab Embed: from n/a through 1.5.	6.5	More Details
CVE-2024-37507	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themewinter Eventin allows Stored XSS.This issue affects Eventin: from n/a through 3.3.57.	6.5	More Details
CVE-2024-37500	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Beaver Builder Team Beaver Builder allows Stored XSS.This issue affects Beaver Builder: from n/a through 2.8.2.2.	6.5	More Details
CVE-2024-38757	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Typebot allows Stored XSS.This issue affects Typebot: from n/a through 3.6.0.	6.5	More Details
CVE-2024-37956	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Vektor,Inc. VK All in One Expansion Unit allows Stored XSS.This issue affects VK All in One Expansion Unit: from n/a through 9.99.1.0.	6.5	More Details
CVE-2024-38741	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Noor-E-Alam Amazing Hover Effects allows Stored XSS.This issue affects Amazing Hover Effects: from n/a through 2.4.9.	6.5	More Details
CVE-2024-38686	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pluginic FancyPost – Best Ultimate Post Block, Post Grid, Layouts, Carousel, Slider For Gutenberg & Elementor allows Stored XSS.This issue affects FancyPost – Best Ultimate Post Block, Post Grid, Layouts, Carousel, Slider For Gutenberg & Elementor: from n/a through 5.3.1.	6.5	More Details
CVE-2024-38682	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Techeshta Post Layouts for Gutenberg allows Stored XSS.This issue affects Post Layouts for Gutenberg: from n/a through 1.2.7.	6.5	More Details
CVE-2024-38681	Improper Neutralization of Input During Web Page Generation (XSS or '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 1.1.41.	6.5	More Details
CVE-2024-38679	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Yongki Agustinus Animated Typed JS Shortcode allows Stored XSS.This issue affects Animated Typed JS Shortcode: from n/a through 2.0.	6.5	More Details
CVE-2024-38678	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Calendar.Online Calendar.Online / Kalender.Digital allows Stored XSS.This issue affects Calendar.Online / Kalender.Digital: from n/a through 1.0.8.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38677	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Reviews.Co.Uk REVIEWS.Io allows Stored XSS.This issue affects REVIEWS.Io: from n/a through 1.2.7.	6.5	More Details
CVE-2024-38676	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Booking Ultra Pro allows Stored XSS.This issue affects Booking Ultra Pro: from n/a through 1.1.13.	6.5	More Details
CVE-2024-38675	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LOOS,Inc. Arkhe Blocks allows Stored XSS.This issue affects Arkhe Blocks: from n/a through 2.22.1.	6.5	More Details
CVE-2024-38674	Improper Neutralization of Input During Web Page Generation (XSS or '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 3.0.	6.5	More Details
CVE-2024-38671	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Martin Gibson WP GoToWebinar allows Stored XSS.This issue affects WP GoToWebinar: from n/a through 15.7.	6.5	More Details
CVE-2024-38670	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Team Members allows Stored XSS.This issue affects Team Members: from n/a through 5.3.3.	6.5	More Details
CVE-2024-37960	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Chris Coyier CodePen Embedded Pens Shortcode allows Stored XSS.This issue affects CodePen Embedded Pens Shortcode: from n/a through 1.0.0.	6.5	More Details
CVE-2024-3934	The Mercado Pago payments for WooCommerce plugin for WordPress is vulnerable to Path Traversal in versions 7.3.0 to 7.5.1 via the mercadopagoDownloadLog function. This makes it possible for authenticated attackers, with subscriber-level access and above, to download and read the contents of arbitrary files on the server, which can contain sensitive information. The arbitrary file download was patched in 7.5.1, while the missing authorization was corrected in version 7.6.2.	6.5	More Details
CVE-2024-29080	Potential vulnerabilities have been identified in the HP Display Control software component within the HP Application Enabling Software Driver which might allow escalation of privilege.	6.5	More Details
CVE-2024-5625	Improper Restriction of XML External Entity Reference vulnerability in PruvaSoft Informatics Apinizer Management Console allows Data Serialization External Entities Blowup.This issue affects Apinizer Management Console: before 2024.05.1.	6.5	More Details
CVE-2024-5620	Authentication Bypass Using an Alternate Path or Channel vulnerability in PruvaSoft Informatics Apinizer Management Console allows Authentication Bypass.This issue affects Apinizer Management Console: before 2024.05.1.	6.5	More Details
CVE-2024-38446	NATO NCI ANET 3.4.1 mishandles report ownership. A user can create a report and, despite the restrictions imposed by the UI, change the author of that report to an arbitrary user (without their consent or knowledge) via a modified UUID in a POST request.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20429	A vulnerability in the web-based management interface of Cisco AsyncOS for Secure Email Gateway could allow an authenticated, remote attacker to execute arbitrary system commands on an affected device. This vulnerability is due to insufficient input validation in certain portions of the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. To successfully exploit this vulnerability, an attacker would need at least valid Operator credentials.	6.5	More Details
CVE-2024-20416	A vulnerability in the upload module of Cisco RV340 and RV345 Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to insufficient boundary checks when processing specific HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the device.	6.5	More Details
CVE-2024-40617	Path traversal vulnerability exists in FUJITSU Network Edgiot GW1500 (M2M-GW for FENICS). If a remote authenticated attacker with User Class privilege sends a specially crafted request to the affected product, access restricted files containing sensitive information may be accessed. As a result, Administrator Class privileges of the product may be hijacked.	6.5	More Details
CVE-2024-38684	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in FunnelKit SlingBlocks – Gutenberg Blocks by FunnelKit (Formerly WooFunnels) allows Stored XSS.This issue affects SlingBlocks – Gutenberg Blocks by FunnelKit (Formerly WooFunnels): from n/a through 1.4.1.	6.5	More Details
CVE-2023-7268	The ArtPlacer Widget WordPress plugin before 2.21.2 does not have authorisation check in place when deleting widgets, allowing ay authenticated users, such as subscriber, to delete arbitrary widgets	6.5	More Details
CVE-2024-38698	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SKT Themes SKT Skill Bar allows Stored XSS.This issue affects SKT Skill Bar: from n/a through 2.0.	6.5	More Details
CVE-2024-38739	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in FameThemes OnePress allows Stored XSS.This issue affects OnePress: from n/a through 2.3.8.	6.5	More Details
CVE-2024-38705	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ElementInvader ElementInvader Addons for Elementor allows Stored XSS.This issue affects ElementInvader Addons for Elementor: from n/a through 1.2.4.	6.5	More Details
CVE-2024-38703	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Xylus Themes WP Event Aggregator allows Stored XSS.This issue affects WP Event Aggregator: from n/a through 1.7.9.	6.5	More Details
CVE-2024-38687	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Techfyd Sky Addons for Elementor allows Stored XSS.This issue affects Sky Addons for Elementor: from n/a through 2.5.5.	6.5	More Details
CVE-2024-38720	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in EazyDocs eazydocs allows Stored XSS.This issue affects EazyDocs: from n/a through 2.5.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38713	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in J.N. Breetvelt a.K.A. OpaJaap WP Photo Album Plus allows Stored XSS.This issue affects WP Photo Album Plus: from n/a through 8.8.02.002.	6.5	More Details
CVE-2024-38722	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PickPlugins Job Board Manager allows Stored XSS.This issue affects Job Board Manager: from n/a through 2.1.57.	6.5	More Details
CVE-2024-38718	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in clicklabs® Medienagentur Download Button for Elementor allows Stored XSS.This issue affects Download Button for Elementor: from n/a through 1.2.1.	6.5	More Details
CVE-2024-38712	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Qode Interactive Qi Blocks allows Stored XSS.This issue affects Qi Blocks: from n/a through 1.3.	6.5	More Details
CVE-2024-38697	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ali Rahimi Goftino allows Stored XSS.This issue affects Goftino: from n/a through 1.6.	6.5	More Details
CVE-2024-5255	The Ultimate Addons for WPBakery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ultimate_dual_color shortcode in all versions up to, and including, 3.19.20 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-2024-5253	The Ultimate Addons for WPBakery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ult_team shortcode in all versions up to, and including, 3.19.20 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-2024-5251	The Ultimate Addons for WPBakery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ultimate_pricing shortcode in all versions up to, and including, 3.19.20 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-2024-5252	The Ultimate Addons for WPBakery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ultimate_info_table shortcode in all versions up to, and including, 3.19.20 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-2024-5582	The Schema & Structured Data for WP & AMP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'url' attribute within the Q&A Block widget in all versions up to, and including, 1.33 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-2024-5554	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘onclick_event’ parameter in all versions up to, and including, 5.6.11 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-2024-5964	The Zenon Lite theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘url’ parameter within the theme's Button shortcode in all versions up to, and including, 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-2024-39682	Cooked is a recipe plugin for WordPress. The Cooked plugin for WordPress is vulnerable to HTML Injection in versions up to, and including, 1.7.15.4 due to insufficient input sanitization and output escaping. This vulnerability allows authenticated attackers with contributor-level access and above to inject arbitrary HTML in pages that will be shown whenever a user accesses a compromised page. This issue has been addressed in release version 1.8.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.4	More Details
CVE-2024-2337	The Easy Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'testimonials_grid ' shortcode in all versions up to, and including, 3.9.5 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-2024-5555	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘social-link-title’ parameter in all versions up to, and including, 5.6.5 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-2024-38723	Server-Side Request Forgery (SSRF) vulnerability in Bernhard Kux JSON Content Importer.This issue affects JSON Content Importer: from n/a through 1.5.6.	6.4	More Details
CVE-2024-41824	In JetBrains TeamCity before 2024.07 parameters of the "password" type could leak into the build log in some specific cases	6.4	More Details
CVE-2024-6848	The Post and Page Builder by BoldGrid – Visual Drag and Drop Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via file uploads in all versions up to, and including, 1.26.6 due to insufficient input sanitization and output escaping affecting the boldgrid_canvas_image AJAX endpoint. 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 the SVG file.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20395	A vulnerability in the media retrieval functionality of Cisco Webex App could allow an unauthenticated, adjacent attacker to gain access to sensitive session information. This vulnerability is due to insecure transmission of requests to backend services when the app accesses embedded media, such as images. An attacker could exploit this vulnerability by sending a message with embedded media that is stored on a messaging server to a targeted user. If the attacker can observe transmitted traffic in a privileged network position, a successful exploit could allow the attacker to capture session token information from insecurely transmitted requests and possibly reuse the captured session information to take further actions as the targeted user.	6.4	More Details
CVE-2024-5254	The Ultimate Addons for WPBakery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ultimate_info_banner shortcode in all versions up to, and including, 3.19.20 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-2024-28796	IBM ClearQuest (CQ) 9.1 through 9.1.0.6 is vulnerable to stored 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: 286833.	6.4	More Details
CVE-2024-6967	A vulnerability was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. It has been classified as critical. This affects an unknown part of the file /employee_gatepass/admin/?page=employee/manage_employee. 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-272121 was assigned to this vulnerability.	6.3	More Details
CVE-2024-6904	A vulnerability, which was classified as critical, was found in SourceCodester Record Management System 1.0. This affects an unknown part of the file sort2_user.php. The manipulation of the argument qualification 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-271929 was assigned to this vulnerability.	6.3	More Details
CVE-2024-6970	A vulnerability classified as critical has been found in itsourcecode Tailoring Management System 1.0. Affected is an unknown function of the file /staffcatadd.php. The manipulation of the argument title 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-272124.	6.3	More Details
CVE-2024-6969	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /ajax/get_patient_history.php. The manipulation of the argument patient_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-272123.	6.3	More Details
CVE-2024-6968	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /print_patients_visits.php. The manipulation of the argument from/to leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-272122 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6956	A vulnerability was found in itsourcecode University Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /view_cgpa.php. The manipulation of the argument VR/VN leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-272078 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-6950	A vulnerability, which was classified as critical, has been found in Prain up to 1.3.0. Affected by this issue is some unknown functionality of the file /?import of the component HTTP POST Request Handler. The manipulation of the argument file leads to code 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-272072.	6.3	More Details
CVE-2024-41124	Puncia is the Official CLI utility for Subdomain Center & Exploit Observer. `API_URLS` is utilizing HTTP instead of HTTPS for communication that can lead to issues like Eavesdropping, Data Tampering, Unauthorized Data Access & MITM Attacks. This issue has been addressed in release version 0.21 by using https rather than http connections. All users are advised to upgrade. There is no known workarounds for this vulnerability.	6.3	More Details
CVE-2024-6905	A vulnerability has been found in SourceCodester Record Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file view_info_user.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-271930 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-6906	A vulnerability was found in SourceCodester Record Management System 1.0 and classified as critical. This issue affects some unknown processing of the file add_leave_non_user.php. The manipulation of the argument LSS 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-271931.	6.3	More Details
CVE-2024-6951	A vulnerability, which was classified as critical, was found in SourceCodester Simple Online Book Store System 1.0. This affects an unknown part of the file admin_delete.php. The manipulation of the argument bookisbn 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-272073 was assigned to this vulnerability.	6.3	More Details
CVE-2024-6944	A vulnerability was found in ZhongBangKeJi CRMEB up to 5.4.0 and classified as critical. Affected by this issue is the function get_image_base64 of the file PublicController.php. The manipulation of the argument file leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-272066 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-2024-6945	A vulnerability was found in Flute CMS 0.2.2.4-alpha. It has been classified as critical. This affects an unknown part of the file app/Core/Http/Controllers/Profile/ImagesController.php of the component Avatar Upload Page. The manipulation of the argument avatar leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272067.	6.3	More Details
CVE-2024-6958	A vulnerability classified as critical was found in itsourcecode University Management System 1.0. This vulnerability affects unknown code of the file /st_update.php of the component Avatar File Handler. The manipulation of the argument personal_image leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272080.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6948	A vulnerability classified as critical has been found in Gargaj wuhu up to 3faad49bfcc3895e9ff76a591d05c8941273d120. Affected is an unknown function of the file /slideeditor.php of the component Slide Editor. The manipulation of the argument newSlideFile leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. VDB-272070 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-6801	A vulnerability, which was classified as critical, has been found in SourceCodester Online Student Management System 1.0. This issue affects some unknown processing of the file /add-students.php. The manipulation of the argument image leads to unrestricted upload. 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-271703.	6.3	More Details
CVE-2024-6903	A vulnerability, which was classified as critical, has been found in SourceCodester Record Management System 1.0. Affected by this issue is some unknown functionality of the file sort1_user.php. The manipulation of the argument position 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-271928.	6.3	More Details
CVE-2024-6902	A vulnerability classified as critical was found in SourceCodester Record Management System 1.0. Affected by this vulnerability is an unknown functionality of the file sort_user.php. The manipulation of the argument sort 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-271927.	6.3	More Details
CVE-2024-6802	A vulnerability, which was classified as critical, was found in SourceCodester Computer Laboratory Management System 1.0. Affected is an unknown function of the file /lms/classes/Master.php?f=save_record. 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.	6.3	More Details
CVE-2024-6933	A vulnerability was found in LimeSurvey 6.5.14-240624. It has been rated as critical. Affected by this issue is the function actionUpdateSurveyLocaleSettingsGeneralSettings of the file /index.php?r=admin/database/index/updatesurveylocalesettings_generalsettings of the component Survey General Settings Handler. The manipulation of the argument language 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-271988. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-41012	In the Linux kernel, the following vulnerability has been resolved: filelock: Remove locks reliably when fcntl/close race is detected When fcntl_setlk() races with close(), it removes the created lock with do_lock_file_wait(). However, LSMs can allow the first do_lock_file_wait() that created the lock while denying the second do_lock_file_wait() that tries to remove the lock. Separately, posix_lock_file() could also fail to remove a lock due to GFP_KERNEL allocation failure (when splitting a range in the middle). After the bug has been triggered, use-after-free reads will occur in lock_get_status() when userspace reads /proc/locks. This can likely be used to read arbitrary kernel memory, but can't corrupt kernel memory. Fix it by calling locks_remove_posix() instead, which is designed to reliably get rid of POSIX locks associated with the given file and files_struct and is also used by filp_flush().	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6830	A vulnerability, which was classified as critical, was found in SourceCodester Simple Inventory Management System 1.0. Affected is an unknown function of the file action.php of the component Order Handler. The manipulation of the argument order_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-271812.	6.3	More Details
CVE-2024-40402	A SQL injection vulnerability was found in 'ajax.php' of Sourcecodester Simple Library Management System 1.0. This vulnerability stems from insufficient user input validation of the 'username' parameter, allowing attackers to inject malicious SQL queries.	6.3	More Details
CVE-2024-6952	A vulnerability has been found in itsourcecode University Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /view_single_result.php?vr=123321&vn=mirage. The manipulation of the argument seme leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-272074 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-6953	A vulnerability was found in itsourcecode Tailoring Management System 1.0 and classified as critical. This issue affects some unknown processing of the file sms.php. The manipulation of the argument customer 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-272075.	6.3	More Details
CVE-2024-6899	A vulnerability was found in SourceCodester Record Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file view_info.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-271924.	6.3	More Details
CVE-2024-6943	A vulnerability has been found in ZhongBangKeJi CRMEB up to 5.4.0 and classified as critical. Affected by this vulnerability is the function downloadImage of the file app/services/product/product/CopyTaobaoServices.php. The manipulation leads to deserialization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272065 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-2024-6900	A vulnerability was found in SourceCodester Record Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file edit_emp.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-271925 was assigned to this vulnerability.	6.3	More Details
CVE-2024-6901	A vulnerability classified as critical has been found in SourceCodester Record Management System 1.0. Affected is an unknown function of the file entry.php. The manipulation of the argument school 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-271926 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-30125	HCL BigFix Compliance server can respond with an HTTP status of 500, indicating a server-side error that may cause the server process to die.	6.2	More Details
CVE-2024-5321	A security issue was discovered in Kubernetes clusters with Windows nodes where BUILTIN\Users may be able to read container logs and NT AUTHORITY\Authenticated Users may be able to modify container logs.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41599	Cross Site Scripting vulnerability in RuoYi v.4.7.9 and before allows a remote attacker to execute arbitrary code via the file upload method	6.1	More Details
CVE-2023-43971	Cross Site Scripting vulnerability in ACG-faka v1.1.7 allows a remote attacker to execute arbitrary code via the encode parameter in Index.php.	6.1	More Details
CVE-2024-38156	Microsoft Edge (Chromium-based) Spoofing Vulnerability	6.1	More Details
CVE-2024-24507	Cross Site Scripting vulnerability in Act-On 2023 allows a remote attacker to execute arbitrary code via the newUser parameter in the login.jsp component.	6.1	More Details
CVE-2024-39090	The PHPGurukul Online Shopping Portal Project version 2.0 contains a vulnerability that allows Cross-Site Request Forgery (CSRF) to lead to Stored Cross-Site Scripting (XSS). An attacker can exploit this vulnerability to execute arbitrary JavaScript code in the context of a user's session, potentially leading to account takeover.	6.1	More Details
CVE-2024-38436	Commugen SOX 365 – CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2024-40347	A reflected cross-site scripting (XSS) vulnerability in Hyland Alfresco Platform 23.2.1-r96 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload into the parameter htmlid.	6.1	More Details
CVE-2024-37551	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Perials Simple Social Share allows Stored XSS.This issue affects Simple Social Share: from n/a through 3.0.	5.9	More Details
CVE-2024-37565	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in TemeGUM Gum Elementor Addon allows Stored XSS.This issue affects Gum Elementor Addon: from n/a through 1.3.5.	5.9	More Details
CVE-2024-37552	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Inisev Social Media & Share Icons allows Stored XSS.This issue affects Social Media & Share Icons: from n/a through 2.9.1.	5.9	More Details
CVE-2024-37556	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SeedProd WordPress Notification Bar allows Stored XSS.This issue affects WordPress Notification Bar: from n/a through 1.3.10.	5.9	More Details
CVE-2024-37434	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Atarim allows Stored XSS.This issue affects Atarim: from n/a through 3.31.	5.9	More Details
CVE-2024-37429	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Hamid Alinia – idehweb Login with phone number allows Stored XSS.This issue affects Login with phone number: from n/a through 1.7.35.	5.9	More Details
CVE-2024-37557	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Soham Web Solution WP Cookie Law Info allows Stored XSS.This issue affects WP Cookie Law Info: from n/a through 1.1.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37558	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Nazmul Hossain Nihal WPFavicon allows Stored XSS.This issue affects WPFavicon: from n/a through 2.1.1.	5.9	More Details
CVE-2024-37239	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPMU DEV Branda allows Stored XSS.This issue affects Branda: from n/a through 3.4.17.	5.9	More Details
CVE-2024-37414	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Depicter Slider and Popup by Averta Depicter Slider allows Stored XSS.This issue affects Depicter Slider: from n/a through 3.0.2.	5.9	More Details
CVE-2024-37409	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Beaver Addons PowerPack Lite for Beaver Builder allows Stored XSS.This issue affects PowerPack Lite for Beaver Builder: from n/a through 1.3.0.4.	5.9	More Details
CVE-2024-37278	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pratik Chaskar Cards for Beaver Builder.This issue affects Cards for Beaver Builder: from n/a through 1.1.4.	5.9	More Details
CVE-2024-37271	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Michael Nelson Print My Blog allows Stored XSS.This issue affects Print My Blog: from n/a through 3.27.0.	5.9	More Details
CVE-2024-37950	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CodexHelp Master Popups allows Stored XSS.This issue affects Master Popups: from n/a through 1.0.3.	5.9	More Details
CVE-2024-39702	In lj_str_hash.c in OpenResty 1.19.3.1 through 1.25.3.1, the string hashing function (used during string interning) allows HashDoS (Hash Denial of Service) attacks. An attacker could cause excessive resource usage during proxy operations via crafted requests, potentially leading to a denial of service with relatively few incoming requests. This vulnerability only exists in the OpenResty fork in the openresty/luajit2 GitHub repository. The LuaJIT/LuaJIT repository. is unaffected.	5.9	More Details
CVE-2024-5604	The Bug Library WordPress plugin before 2.1.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	5.9	More Details
CVE-2024-37947	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themeum Tutor LMS allows Stored XSS.This issue affects Tutor LMS: from n/a through 2.7.2.	5.9	More Details
CVE-2024-37561	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jamie Bergen Plugin Notes Plus allows Stored XSS.This issue affects Plugin Notes Plus: from n/a through 1.2.6.	5.9	More Details
CVE-2024-37120	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Biplob Adhikari Tabs allows Stored XSS.This issue affects Tabs: from n/a through 4.0.6.	5.9	More Details
CVE-2024-38710	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jewel Theme Master Addons for Elementor allows Stored XSS.This issue affects Master Addons for Elementor: from n/a through 2.0.6.2.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37121	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in biplob018 Shortcode Addons allows Stored XSS.This issue affects Shortcode Addons: from n/a through 3.2.5.	5.9	More Details
CVE-2024-6833	A vulnerability in Zowe CLI allows local, privileged actors to store previously entered secure credentials in a plaintext file as part of an auto-init operation.	5.9	More Details
CVE-2024-6231	The Request a Quote WordPress plugin before 2.4.1 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)	5.9	More Details
CVE-2024-38738	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Marian Kadanka Change From Email allows Stored XSS.This issue affects Change From Email: from n/a through 1.2.1.	5.9	More Details
CVE-2024-38725	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Webstix Admin Dashboard RSS Feed allows Stored XSS.This issue affects Admin Dashboard RSS Feed: from n/a through 3.1.	5.9	More Details
CVE-2024-37523	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AMP-MODE Login Logo Editor allows Stored XSS.This issue affects Login Logo Editor: from n/a through 1.3.3.	5.9	More Details
CVE-2024-37536	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Web357 Easy Custom Code (LESS/CSS/JS) – Live editing allows Stored XSS.This issue affects Easy Custom Code (LESS/CSS/JS) – Live editing: from n/a through 1.0.8.	5.9	More Details
CVE-2024-37537	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in UusWeb.Ee WS Contact Form allows Stored XSS.This issue affects WS Contact Form: from n/a through 1.3.7.	5.9	More Details
CVE-2024-37538	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Thomas Kuhlmann Link To Bible allows Stored XSS.This issue affects Link To Bible: from n/a through 2.5.9.	5.9	More Details
CVE-2024-37545	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Nick Halsey Floating Social Media Links allows Stored XSS.This issue affects Floating Social Media Links: from n/a through 1.5.2.	5.9	More Details
CVE-2024-37562	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BracketSpace Simple Post Notes allows Stored XSS.This issue affects Simple Post Notes: from n/a through 1.7.7.	5.9	More Details
CVE-2024-37548	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Meks Meks Easy Ads Widget allows Stored XSS.This issue affects Meks Easy Ads Widget: from n/a through 2.0.8.	5.9	More Details
CVE-2024-37549	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pdfcrowd Save as PDF plugin by Pdfcrowd allows Stored XSS.This issue affects Save as PDF plugin by Pdfcrowd: from n/a through 4.0.0.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37215	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in creativeinteractivemedia Transition Slider – Responsive Image Slider and Gallery allows Stored XSS.This issue affects Transition Slider – Responsive Image Slider and Gallery: from n/a through 2.20.3.	5.9	More Details
CVE-2024-37550	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Envato Template Kit – Export allows Stored XSS.This issue affects Template Kit – Export: from n/a through 1.0.22.	5.9	More Details
CVE-2024-37122	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Biplob Adhikari Accordions allows Stored XSS.This issue affects Accordions: from n/a through 2.3.5.	5.9	More Details
CVE-2024-37946	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in weDevs ReCaptcha Integration for WordPress allows Stored XSS.This issue affects ReCaptcha Integration for WordPress: from n/a through 1.2.5.	5.9	More Details
CVE-2024-29120	In Streampark (version < 2.1.4), when a user logged in successfully, the Backend service would return "Authorization" as the front-end authentication credential. User can use this credential to request other users' information, including the administrator's username, password, salt value, etc. Mitigation: all users should upgrade to 2.1.4	5.9	More Details
CVE-2024-37522	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Dario Curasì CC & BCC for Woocommerce Order Emails allows Stored XSS.This issue affects CC & BCC for Woocommerce Order Emails: from n/a through 1.4.1.	5.9	More Details
CVE-2024-38689	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Garrett Grimm Simple Popup allows Stored XSS.This issue affects Simple Popup: from n/a through 4.4.	5.9	More Details
CVE-2024-37919	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pratik Chaskar Timeline Module for Beaver Builder allows Stored XSS.This issue affects Timeline Module for Beaver Builder: from n/a through 1.1.3.	5.9	More Details
CVE-2024-37446	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kiboko Labs Chained Quiz allows Stored XSS.This issue affects Chained Quiz: from n/a through 1.3.2.8.	5.9	More Details
CVE-2024-37447	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PixelYourSite PixelYourSite – Your smart PIXEL (TAG) Manager allows Stored XSS.This issue affects PixelYourSite – Your smart PIXEL (TAG) Manager: from n/a through 9.6.1.1.	5.9	More Details
CVE-2024-37449	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemePunch OHG Slider Revolution.This issue affects Slider Revolution: from n/a through 6.7.13.	5.9	More Details
CVE-2024-38784	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Livemesh Livemesh Addons for Beaver Builder allows Stored XSS.This issue affects Livemesh Addons for Beaver Builder: from n/a through 3.6.1.	5.9	More Details
CVE-2024-6916	A vulnerability in Zowe CLI allows local, privileged actors to display securely stored properties in cleartext within a terminal using the '--show-inputs-only' flag.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38685	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SubscriptionPro WP Announcement allows Stored XSS.This issue affects WP Announcement: from n/a through 2.0.8.	5.9	More Details
CVE-2024-6961	RAIL documents are an XML-based format invented by Guardrails AI to enforce formatting checks on LLM outputs. Guardrails users that consume RAIL documents from external sources are vulnerable to XXE, which may cause leakage of internal file data via the SYSTEM entity.	5.9	More Details
CVE-2024-37943	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in YITH YITH WooCommerce Ajax Product Filter allows Reflected XSS.This issue affects YITH WooCommerce Ajax Product Filter: from n/a through 5.1.0.	5.8	More Details
CVE-2024-37515	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Optemiz XPlainer - WooCommerce Product FAQ allows Reflected XSS.This issue affects XPlainer - WooCommerce Product FAQ: from n/a through 1.6.3.	5.8	More Details
CVE-2024-27311	Zohocorp ManageEngine DDI Central versions 4001 and prior were vulnerable to directory traversal vulnerability which allows the user to upload new files to the server folder.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41009	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix overrunning reservations in ringbuf The BPF ring buffer internally is implemented as a power-of-2 sized circular buffer, with two logical and ever-increasing counters: consumer_pos is the consumer counter to show which logical position the consumer consumed the data, and producer_pos which is the producer counter denoting the amount of data reserved by all producers. Each time a record is reserved, the producer that "owns" the record will successfully advance producer counter. In user space each time a record is read, the consumer of the data advanced the consumer counter once it finished processing. Both counters are stored in separate pages so that from user space, the producer counter is read-only and the consumer counter is read-write. One aspect that simplifies and thus speeds up the implementation of both producers and consumers is how the data area is mapped twice contiguously back-to-back in the virtual memory, allowing to not take any special measures for samples that have to wrap around at the end of the circular buffer data area, because the next page after the last data page would be first data page again, and thus the sample will still appear completely contiguous in virtual memory. Each record has a struct bpf_ringbuf_hdr { u32 len; u32 pg_off; } header for book-keeping the length and offset, and is inaccessible to the BPF program. Helpers like bpf_ringbuf_reserve() return `(void *)hdr + BPF_RINGBUF_HDR_SZ` for the BPF program to use. Bing-Jhong and Muhammad reported that it is however possible to make a second allocated memory chunk overlapping with the first chunk and as a result, the BPF program is now able to edit first chunk's header. For example, consider the creation of a BPF_MAP_TYPE_RINGBUF map with size of 0x4000. Next, the consumer_pos is modified to 0x3000 /before/ a call to bpf_ringbuf_reserve() is made. This will allocate a chunk A, which is in [0x0,0x3008], and the BPF program is able to edit [0x8,0x3008]. Now, lets allocate a chunk B with size 0x3000. This will succeed because consumer_pos was edited ahead of time to pass the `new_prod_pos - cons_pos > rb->mask` check. Chunk B will be in range [0x3008,0x6010], and the BPF program is able to edit [0x3010,0x6010]. Due to the ring buffer memory layout mentioned earlier, the ranges [0x0,0x4000] and [0x4000,0x8000] point to the same data pages. This means that chunk B at [0x4000,0x4008] is chunk A's header. bpf_ringbuf_submit() / bpf_ringbuf_discard() use the header's pg_off to then locate the bpf_ringbuf itself via bpf_ringbuf_restore_from_rec(). Once chunk B modified chunk A's header, then bpf_ringbuf_commit() refers to the wrong page and could cause a crash. Fix it by calculating the oldest pending_pos and check whether the range from the oldest outstanding record to the newest would span beyond the ring buffer size. If that is the case, then reject the request. We've tested with the ring buffer benchmark in BPF selftests (./benchs/run_bench_ringbufs.sh) before/after the fix and while it seems a bit slower on some benchmarks, it is still not significantly enough to matter.	5.5	More Details
CVE-2024-6638	An integer overflow vulnerability due to improper input validation when reading TDMS files in LabVIEW may result in an infinite loop. Successful exploitation requires an attacker to provide a user with a specially crafted TDMS file. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	5.5	More Details
CVE-2024-6803	A vulnerability has been found in itsourcecode Document Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file insert.php. The manipulation of the argument anothercont 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-271705 was assigned to this vulnerability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6705	The RegLevel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.2.1 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.	5.5	More Details
CVE-2024-41836	InDesign Desktop versions ID18.5.2, ID19.3 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS) condition. An attacker could exploit this vulnerability to crash the application, resulting in a DoS. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-41665	Ampache, a web based audio/video streaming application and file manager, has a stored cross-site scripting (XSS) vulnerability in versions prior to 6.6.0. This vulnerability exists in the "Playlists - Democratic - Configure Democratic Playlist" feature. An attacker with Content Manager permissions can set the Name field to `<svg onload=alert(8)>`. When any administrator or user accesses the Democratic functionality, they will be affected by this stored XSS vulnerability. The attacker can exploit this vulnerability to obtain the cookies of any user or administrator who accesses the `democratic.php` file. Version 6.6.0 contains a patch for the issue.	5.5	More Details
CVE-2024-6122	An incorrect permission in the installation directory for the shared NI SystemLink Server KeyValueDatabase service may result in information disclosure via local access. This affects NI SystemLink Server 2024 Q1 and prior versions. It also affects NI FlexLogger 2023 Q2 and prior versions which installed this shared service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41010	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix too early release of tcx_entry Pedro Pinto and later independently also Hyunwoo Kim and Wongi Lee reported an issue that the tcx_entry can be released too early leading to a use after free (UAF) when an active old-style ingress or clsact qdisc with a shared tc block is later replaced by another ingress or clsact instance. Essentially, the sequence to trigger the UAF (one example) can be as follows: 1. A network namespace is created 2. An ingress qdisc is created. This allocates a tcx_entry, and &tcx_entry->miniq is stored in the qdisc's miniqp->p_miniq. At the same time, a tcf block with index 1 is created. 3. chain0 is attached to the tcf block. chain0 must be connected to the block linked to the ingress qdisc to later reach the function tcf_chain0_head_change_cb_del() which triggers the UAF. 4. Create and graft a clsact qdisc. This causes the ingress qdisc created in step 1 to be removed, thus freeing the previously linked tcx_entry: rtnetlink_rcv_msg() => tc_modify_qdisc() => qdisc_create() => clsact_init() [a] => qdisc_graft() => qdisc_destroy() => __qdisc_destroy() => ingress_destroy() [b] => tcx_entry_free() => kfree_rcu() // tcx_entry freed 5. Finally, the network namespace is closed. This registers the cleanup_net worker, and during the process of releasing the remaining clsact qdisc, it accesses the tcx_entry that was already freed in step 4, causing the UAF to occur: cleanup_net() => ops_exit_list() => default_device_exit_batch() => unregister_netdevice_many() => unregister_netdevice_many_notify() => dev_shutdown() => qdisc_put() => clsact_destroy() [c] => tcf_block_put_ext() => tcf_chain0_head_change_cb_del() => tcf_chain_head_change_item() => clsact_chain_head_change() => mini_qdisc_pair_swap() // UAF There are also other variants, the gist is to add an ingress (or clsact) qdisc with a specific shared block, then to replace that qdisc, waiting for the tcx_entry kfree_rcu() to be executed and subsequently accessing the current active qdisc's miniq one way or another. The correct fix is to turn the miniq_active boolean into a counter. What can be observed, at step 2 above, the counter transitions from 0->1, at step [a] from 1->2 (in order for the miniq object to remain active during the replacement), then in [b] from 2->1 and finally [c] 1->0 with the eventual release. The reference counter in general ranges from [0,2] and it does not need to be atomic since all access to the counter is protected by the rtnl mutex. With this in place, there is no longer a UAF happening and the tcx_entry is freed at the correct time.	5.5	More Details
CVE-2024-6669	The AI ChatBot for WordPress – WPBot plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 5.5.7 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.	5.5	More Details
CVE-2024-39863	Apache Airflow versions before 2.9.3 have a vulnerability that allows an authenticated attacker to inject a malicious link when installing a provider. Users are recommended to upgrade to version 2.9.3, which fixes this issue.	5.4	More Details
CVE-2024-39124	In Roundup before 2.4.0, classhelpers (_generic.help.html) allow XSS.	5.4	More Details
CVE-2024-39457	Cybozu Garoon 6.0.0 to 6.0.1 contains a cross-site scripting vulnerability in PDF preview. If this vulnerability is exploited, an arbitrary script may be executed on a logged-in user’s web browser.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32981	Silverstripe framework is the PHP framework forming the base for the Silverstripe CMS. In affected versions a bad actor with access to edit content in the CMS could add send a specifically crafted encoded payload to the server, which could be used to inject a JavaScript payload on the front end of the site. The payload would be sanitised on the client-side, but server-side sanitisation doesn't catch it. The server-side sanitisation logic has been updated to sanitise against this type of attack in version 5.2.16. All users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2024-6175	The Booking Ultra Pro Appointments Booking Calendar Plugin plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the multiple functions in all versions up to, and including, 1.1.13. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify and delete. multiple plugin options and data such as payments, pricing, booking information, business hours, calendars, profile information, and email templates.	5.4	More Details
CVE-2024-39680	Cooked is a recipe plugin for WordPress. The Cooked plugin for WordPress is vulnerable to Cross-Site Request Forgery (CSRF) in versions up to, and including, 1.7.15.4 due to missing or incorrect nonce validation on the AJAX action handler. This vulnerability could allow an attacker to trick users into performing an action they didn't intend to perform under their current authentication. This issue has been addressed in release version 1.8.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2024-6271	The Community Events WordPress plugin before 1.5 does not have CSRF check in place when deleting events, which could allow attackers to make a logged in admin delete arbitrary events via a CSRF attack	5.4	More Details
CVE-2024-38503	When editing a user, group or any object in the Syncope Console, HTML tags could be added to any text field and could lead to potential exploits. The same vulnerability was found in the Syncope Enduser, when editing “Personal Information” or “User Requests”. Users are recommended to upgrade to version 3.0.8, which fixes this issue.	5.4	More Details
CVE-2024-40648	matrix-rust-sdk is an implementation of a Matrix client-server library in Rust. The `UserIdentity::is_verified()` method in the matrix-sdk-crypto crate before version 0.7.2 doesn't take into account the verification status of the user's own identity while performing the check and may as a result return a value contrary to what is implied by its name and documentation. If the method is used to decide whether to perform sensitive operations towards a user identity, a malicious homeserver could manipulate the outcome in order to make the identity appear trusted. This is not a typical usage of the method, which lowers the impact. The method itself is not used inside the `matrix-sdk-crypto` crate. The 0.7.2 release of the `matrix-sdk-crypto` crate includes a fix. All users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2024-5977	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.13.0 via the 'handleRequest' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with GiveWP Worker-level access and above, to delete and update arbitrary posts.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41664	Canarytokens help track activity and actions on a network. Prior to `sha-8ea5315`, Canarytokens.org was vulnerable to a blind SSRF in the Webhook alert feature. When a Canarytoken is created, users choose to receive alerts either via email or via a webhook. If a webhook is supplied when a Canarytoken is first created, the site will make a test request to the supplied URL to ensure it accepts alert notification HTTP requests. No safety checks were performed on the URL, leading to a Server-Side Request Forgery vulnerability. The SSRF is Blind because the content of the response is not displayed to the creating user; they are simply told whether an error occurred in making the test request. Using the Blind SSRF, it was possible to map out open ports for IPs inside the Canarytokens.org infrastructure. This issue is now patched on Canarytokens.org. Users of self-hosted Canarytokens installations can update by pulling the latest Docker image, or any Docker image after `sha-097d91a`.	5.4	More Details
CVE-2024-39681	Cooked is a recipe plugin for WordPress. The Cooked plugin for WordPress is vulnerable to Cross-Site Request Forgery (CSRF) in versions up to, and including, 1.7.15.4 due to missing or incorrect nonce validation on the AJAX action handler. This vulnerability could allow an attacker to trick users into performing an action they didn't intend to perform under their current authentication. This issue has been addressed in release version 1.8.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2024-39123	In janeczku Calibre-Web 0.6.0 to 0.6.21, the edit_book_comments function is vulnerable to Cross Site Scripting (XSS) due to improper sanitization performed by the clean_string function. The vulnerability arises from the way the clean_string function handles HTML sanitization.	5.4	More Details
CVE-2024-38759	Deserialization of Untrusted Data vulnerability in WP MEDIA SAS Search & Replace search-and-replace.This issue affects Search & Replace: from n/a through 3.2.2.	5.4	More Details
CVE-2024-34128	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-41130	llama.cpp provides LLM inference in C/C++. Prior to b3427, llama.cpp contains a null pointer dereference in gguf_init_from_file. This vulnerability is fixed in b3427.	5.4	More Details
CVE-2024-39126	Roundup before 2.4.0 allows XSS via JavaScript in PDF, XML, and SVG documents.	5.4	More Details
CVE-2024-39125	Roundup before 2.4.0 allows XSS via a SCRIPT element in an HTTP Referer header.	5.4	More Details
CVE-2023-6708	The SVG Support plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the SVG upload feature in all versions up to, and including, 2.5.5 due to insufficient input sanitization and output escaping, even when the 'Sanitize SVG while uploading' feature is enabled. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Note that successful exploitation of this vulnerability requires the administrator to allow author-level users to upload SVG files.	5.4	More Details
CVE-2024-41880	In veilid-core in Veilid before 0.3.4, the protocol's ping function can be misused in a way that decreases the effectiveness of safety and private routes.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29073	An vulnerability in the handling of Latex exists in Ankitects Anki 24.04. When Latex is sanitized to prevent unsafe commands, the verbatim package, which comes installed by default in many Latex distributions, has been overlooked. A specially crafted flashcard can lead to an arbitrary file read. An attacker can share a flashcard to trigger this vulnerability.	5.3	More Details
CVE-2024-6560	The Addonify – Quick View For WooCommerce plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.2.16. This is due the plugin utilizing mobiledetect without preventing direct access to the files. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2024-40636	Steeltoe is an open source project that provides a collection of libraries that helps users build production-grade cloud-native applications using externalized configuration, service discovery, distributed tracing, application management, and more. When utilizing multiple Eureka server service URLs with basic auth and encountering an issue with fetching the service registry, an error is logged with the Eureka server service URLs but only the first URL is masked. The code in question is `_logger.LogError(e, "FetchRegistry Failed for Eureka service urls: {EurekaServerServiceUrls}", new Uri(ClientConfig.EurekaServerServiceUrls).ToMaskedString());` in the `DiscoveryClient.cs` file which may leak credentials into logs. This issue has been addressed in version 3.2.8 of the Steeltoe.Discovery.Eureka nuget package.	5.3	More Details
CVE-2024-40725	A partial fix for CVE-2024-39884 in the core of Apache HTTP Server 2.4.61 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP scripts may be served instead of interpreted. Users are recommended to upgrade to version 2.4.62, which fixes this issue.	5.3	More Details
CVE-2024-6535	A flaw was found in Skupper. When Skupper is initialized with the console-enabled and with console-auth set to Openshift, it configures the openshift oauth-proxy with a static cookie-secret. In certain circumstances, this may allow an attacker to bypass authentication to the Skupper console via a specially-crafted cookie.	5.3	More Details
CVE-2024-40633	Sylius is an Open Source eCommerce Framework on Symfony. A security vulnerability was discovered in the `/api/v2/shop/adjustments/{id}` endpoint, which retrieves order adjustments based on incremental integer IDs. The vulnerability allows an attacker to enumerate valid adjustment IDs and retrieve order tokens. Using these tokens, an attacker can access guest customer order details - sensitive guest customer information. The issue is fixed in versions: 1.12.19, 1.13.4 and above. The `/api/v2/shop/adjustments/{id}` will always return `404` status. Users are advised to upgrade. Users unable to upgrade may alter their config to mitigate this issue. Please see the linked GHSA for details.	5.3	More Details
CVE-2024-40647	sentry-sdk is the official Python SDK for Sentry.io. A bug in Sentry's Python SDK < 2.8.0 allows the environment variables to be passed to subprocesses despite the `env={}` setting. In Python's `subprocess` calls, all environment variables are passed to subprocesses by default. However, if you specifically do not want them to be passed to subprocesses, you may use `env` argument in `subprocess` calls. Due to the bug in Sentry SDK, with the Stdlib integration enabled (which is enabled by default), this expectation is not fulfilled, and all environment variables are being passed to subprocesses instead. The issue has been patched in pull request #3251 and is included in sentry-sdk==2.8.0. We strongly recommend upgrading to the latest SDK version. However, if it's not possible, and if passing environment variables to child processes poses a security risk for you, you can disable all default integrations.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6489	The Getwid – Gutenberg Blocks plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the get_google_api_key function in all versions up to, and including, 2.0.10. This makes it possible for authenticated attackers, with Contributor-level access and above, to set the MailChimp API key.	5.3	More Details
CVE-2024-41132	ImageSharp is a 2D graphics API. A vulnerability discovered in the ImageSharp library, where the processing of specially crafted files can lead to excessive memory usage in the Gif decoder. The vulnerability is triggered when ImageSharp attempts to process image files that are designed to exploit this flaw. All users are advised to upgrade to v3.1.5 or v2.1.9.	5.3	More Details
CVE-2024-20396	A vulnerability in the protocol handlers of Cisco Webex App could allow an unauthenticated, remote attacker to gain access to sensitive information. This vulnerability exists because the affected application does not safely handle file protocol handlers. An attacker could exploit this vulnerability by persuading a user to follow a link that is designed to cause the application to send requests. If the attacker can observe transmitted traffic in a privileged network position, a successful exploit could allow the attacker to capture sensitive information, including credential information, from the requests.	5.3	More Details
CVE-2024-6455	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 3.2.0 due to a missing capability checks on ekit_widgetarea_content function. This makes it possible for unauthenticated attackers to view any item created in Elementor, such as posts, pages and templates including drafts, pending and private items.	5.3	More Details
CVE-2024-38730	Server-Side Request Forgery (SSRF) vulnerability in Noor alam Magical Addons For Elementor.This issue affects Magical Addons For Elementor: from n/a through 1.1.41.	4.9	More Details
CVE-2024-30473	Dell ECS, versions prior to 3.8.1, contain a privilege elevation vulnerability in user management. A remote high privileged attacker could potentially exploit this vulnerability, gaining access to unauthorized end points.	4.9	More Details
CVE-2024-38758	Server-Side Request Forgery (SSRF) vulnerability in WappPress Team WappPress.This issue affects WappPress: from n/a through 6.0.4.	4.9	More Details
CVE-2024-6243	The HTML Forms WordPress plugin before 1.3.33 does not sanitize and escape the form message inputs, allowing high-privilege users, such as administrators, to perform Stored Cross-Site Scripting (XSS) attacks even when the unfiltered_html capability is disabled.	4.8	More Details
CVE-2024-5529	The WP QuickLaTeX WordPress plugin before 3.8.8 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-2024-5004	The CM Popup Plugin for WordPress WordPress plugin before 1.6.6 does not sanitise and escape some of the campaign settings, which could allow high privilege users such as contributor to perform Stored Cross-Site Scripting attacks	4.8	More Details
CVE-2024-41709	Backdrop CMS before 1.27.3 and 1.28.x before 1.28.2 does not sufficiently sanitize field labels before they are displayed in certain places. This vulnerability is mitigated by the fact that an attacker must have a role with the "administer fields" permission.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6783	A vulnerability has been discovered in Vue, that allows an attacker to perform XSS via prototype pollution. The attacker could change the prototype chain of some properties such as `Object.prototype.staticClass` or `Object.prototype.staticStyle` to execute arbitrary JavaScript code.	4.8	More Details
CVE-2024-39902	Tuleap is an open source suite to improve management of software developments and collaboration. Prior to Tuleap Community Edition 15.10.99.128 and Tuleap Enterprise Edition 15.10-6 and 15.9-8, the checkbox "Apply same permissions to all sub-items of this folder" in the document manager permissions modal is not taken into account and always considered as unchecked. In situations where the permissions are being restricted some users might still keep, incorrectly, the possibility to edit or manage items. Only change made via the web UI are affected, changes directly made via the REST API are not impacted. This vulnerability is fixed in Tuleap Community Edition 15.10.99.128 and Tuleap Enterprise Edition 15.10-6 and 15.9-8.	4.8	More Details
CVE-2024-6947	A vulnerability was found in Flute CMS 0.2.2.4-alpha. It has been rated as critical. This issue affects the function replaceContent of the file app/Core/Support/ContentParser.php of the component Notification Handler. The manipulation leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272069 was assigned to this vulnerability.	4.7	More Details
CVE-2024-29737	In streampark, the project module integrates Maven's compilation capabilities. The input parameter validation is not strict, allowing attackers to insert commands for remote command execution, The prerequisite for a successful attack is that the user needs to log in to the streampark system and have system-level permissions. Generally, only users of that system have the authorization to log in, and users would not manually input a dangerous operation command. Therefore, the risk level of this vulnerability is very low. Mitigation: all users should upgrade to 2.1.4 Background info: Log in to Streampark using the default username (e.g. test1, test2, test3) and the default password (streampark). Navigate to the Project module, then add a new project. Enter the git repository address of the project and input `touch /tmp/success_2.1.2` as the "Build Argument". Note that there is no verification and interception of the special character "`". As a result, you will find that this injection command will be successfully executed after executing the build. In the latest version, the special symbol ` is intercepted.	4.7	More Details
CVE-2023-52291	In streampark, the project module integrates Maven's compilation capabilities. The input parameter validation is not strict, allowing attackers to insert commands for remote command execution, The prerequisite for a successful attack is that the user needs to log in to the streampark system and have system-level permissions. Generally, only users of that system have the authorization to log in, and users would not manually input a dangerous operation command. Therefore, the risk level of this vulnerability is very low. Background: In the "Project" module, the maven build args “<” operator causes command injection. e.g : “< (curl http://xxx.com)” will be executed as a command injection, Mitigation: all users should upgrade to 2.1.4, The "<" operator will blocked。	4.7	More Details
CVE-2024-20400	A vulnerability in the web-based management interface of Cisco Expressway Series could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of HTTP request parameters. An attacker could exploit this vulnerability by intercepting and modifying an HTTP request from a user. A successful exploit could allow the attacker to redirect the user to a malicious web page. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6946	A vulnerability was found in Flute CMS 0.2.2.4-alpha. It has been declared as critical. This vulnerability affects unknown code of the file /admin/pages/list. The manipulation of the argument blocks leads to code 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-272068.	4.7	More Details
CVE-2024-6940	A vulnerability was found in DedeCMS 5.7.114. It has been classified as critical. This affects an unknown part of the file article_template_rand.php. The manipulation leads to code 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-271995. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-30126	HCL BigFix Compliance is affected by a missing X-Frame-Options HTTP header which can allow an attacker to create a malicious website that embeds the target website in a frame or iframe, tricking users into performing actions on the target website without their knowledge.	4.7	More Details
CVE-2024-20296	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to upload arbitrary files to an affected device. To exploit this vulnerability, an attacker would need at least valid Policy Admin credentials on the affected device. This vulnerability is due to improper validation of files that are uploaded to the web-based management interface. An attacker could exploit this vulnerability by uploading arbitrary files to an affected device. A successful exploit could allow the attacker to store malicious files on the system, execute arbitrary commands on the operating system, and elevate privileges to root.	4.7	More Details
CVE-2024-41825	In JetBrains TeamCity before 2024.07 stored XSS was possible on the Code Inspection tab	4.6	More Details
CVE-2023-40539	Philips Vue PACS does not require that users have strong passwords, which could make it easier for attackers to compromise user accounts.	4.4	More Details
CVE-2024-41129	The ops library is a Python framework for developing and testing Kubernetes and machine charms. The issue here is that ops passes the secret content as one of the args via CLI. This issue may affect any of the charms that are using: Juju (>=3.0), Juju secrets and not correctly capturing and processing `subprocess.CalledProcessError`. This vulnerability is fixed in 2.15.0.	4.4	More Details
CVE-2023-40223	Philips Vue PACS does not properly assign, modify, track, or check actor privileges, creating an unintended sphere of control for that actor.	4.4	More Details
CVE-2024-6949	A vulnerability classified as problematic was found in Gargaj wuhu up to 3faad49bfcc3895e9ff76a591d05c8941273d120. Affected by this vulnerability is an unknown functionality of the file /pages.php?edit=News. The manipulation leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-272071.	4.3	More Details
CVE-2024-40075	Laravel v11.x was discovered to contain an XML External Entity (XXE) vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31979	Server-Side Request Forgery (SSRF) vulnerability in Apache StreamPipes during installation process of pipeline elements. Previously, StreamPipes allowed users to configure custom endpoints from which to install additional pipeline elements. These endpoints were not properly validated, allowing an attacker to get StreamPipes to send an HTTP GET request to an arbitrary address. This issue affects Apache StreamPipes: through 0.93.0. Users are recommended to upgrade to version 0.95.0, which fixes the issue.	4.3	More Details
CVE-2024-6799	The YITH Essential Kit for WooCommerce #1 plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'activate_module', 'deactivate_module', and 'install_module' functions in all versions up to, and including, 2.34.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install, activate, and deactivate plugins from a pre-defined list of available YITH plugins.	4.3	More Details
CVE-2024-39679	Cooked is a recipe plugin for WordPress. The Cooked plugin for WordPress is vulnerable to Cross-Site Request Forgery (CSRF) in versions up to, and including, 1.7.15.4 due to missing or incorrect nonce validation on the AJAX action handler. This vulnerability could allow an attacker to trick users into performing an action they didn't intend to perform under their current authentication. This issue has been addressed in release version 1.8.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2024-6033	The Event Manager, Events Calendar, Tickets, Registrations – Eventin plugin for WordPress is vulnerable to unauthorized data importation due to a missing capability check on the 'import_file' function in all versions up to, and including, 4.0.4. This makes it possible for authenticated attackers, with Contributor-level access and above, to import events, speakers, schedules and attendee data.	4.3	More Details
CVE-2024-5804	The Conditional Fields for Contact Form 7 plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.4.13. This is due to missing or incorrect nonce validation on the wpcf7cf_admin_init function. This makes it possible for unauthenticated attackers to reset 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-2024-29885	silverstripe/reports is an API for creating backend reports in the Silverstripe Framework. In affected versions reports can be accessed by their direct URL by any user who has access to view the reports admin section, even if the `canView()` method for that report returns `false`. This issue has been addressed in version 5.2.3. All users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2024-38701	Authorization Bypass Through User-Controlled Key vulnerability in Academy LMS.This issue affects Academy LMS: from n/a through 2.0.4.	4.3	More Details
CVE-2024-39678	Cooked is a recipe plugin for WordPress. The Cooked plugin is vulnerable to Cross-Site Request Forgery (CSRF) in versions up to, and including, 1.7.15.4 due to missing or incorrect nonce validation on the AJAX action handler. This vulnerability could allow an attacker to trick users into performing an action they didn't intend to perform under their current authentication. This issue has been addressed in release version 1.8.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2024-5703	The Email Subscribers by Icegram Express – Email Marketing, Newsletters, Automation for WordPress & WooCommerce plugin for WordPress is vulnerable to unauthorized API access due to a missing capability check in all versions up to, and including, 5.7.26. This makes it possible for authenticated attackers, with Subscriber-level access and above, to access the API (provided it is enabled) and add, edit, and delete audience users.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6599	The Meks Video Importer plugin for WordPress is vulnerable to unauthorized API key modification due to a missing capability check on the ajax_save_settings function in all versions up to, and including, 1.0.11. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify the plugin's API keys	4.3	More Details
CVE-2024-6504	Rapid7 InsightVM Console versions below 6.6.260 suffer from a protection mechanism failure whereby an attacker with network access to the InsightVM Console can cause it to overload or crash by sending repeated invalid REST requests in a short timeframe, to the Console's port 443 causing the console to enter an exception handling logging loop, exhausting the CPU. There is no indication that an attacker can use this method to escalate privilege, acquire unauthorized access to data, or gain control of protected resources. This issue is fixed in version 6.6.261.	4.3	More Details
CVE-2024-6491	The Getwid – Gutenberg Blocks plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the mailchimp_api_key_manage function in all versions up to, and including, 2.0.10. This makes it possible for authenticated attackers, with Contributor-level access and above, to set the MailChimp API key.	4.3	More Details
CVE-2024-5997	The Duplica – Duplicate Posts, Pages, Custom Posts or Users plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the duplicate_user and duplicate_post functions in all versions up to, and including, 0.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create duplicates of users and posts/pages.	4.3	More Details
CVE-2024-41597	Cross Site Request Forgery vulnerability in ProcessWire v.3.0.229 allows a remote attacker to execute arbitrary code via a crafted HTML file to the comments functionality.	4.2	More Details
CVE-2024-21583	Versions of the package github.com/gitpod-io/gitpod/components/server/go/pkg/lib before main-gha.27122; versions of the package github.com/gitpod-io/gitpod/components/ws-proxy/pkg/proxy before main-gha.27122; versions of the package github.com/gitpod-io/gitpod/install/installer/pkg/components/auth before main-gha.27122; versions of the package github.com/gitpod-io/gitpod/install/installer/pkg/components/public-api-server before main-gha.27122; versions of the package github.com/gitpod-io/gitpod/install/installer/pkg/components/server before main-gha.27122; versions of the package @gitpod/gitpod-protocol before 0.1.5-main-gha.27122 are vulnerable to Cookie Tossing due to a missing __Host- prefix on the _gitpod_io_jwt2_ session cookie. This allows an adversary who controls a subdomain to set the value of the cookie on the Gitpod control plane, which can be assigned to an attacker's own JWT so that specific actions taken by the victim (such as connecting a new Github organization) are actioned by the attackers session.	4.1	More Details
CVE-2024-38806	Failure to properly synchronize user's permissions in UAA in Cloud Foundry Foundation v40.17.0 https://github.com/cloudfoundry/cf-deployment/releases/tag/v40.17.0 , potentially resulting in users retaining access rights they should not have. This can allow them to perform operations beyond their intended permissions.	3.9	More Details
CVE-2024-30130	HCL Nomad server on Domino is vulnerable to the cache containing sensitive information which could potentially give an attacker the ability to acquire the sensitive information.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30471	Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Apache StreamPipes in user self-registration. This allows an attacker to potentially request the creation of multiple accounts with the same email address until the email address is registered, creating many identical users and corrupting StreamPipe's user management. This issue affects Apache StreamPipes: through 0.93.0. Users are recommended to upgrade to version 0.95.0, which fixes the issue.	3.7	More Details
CVE-2024-41839	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could lead to a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect the integrity of the page. Exploitation of this issue requires user interaction.	3.5	More Details
CVE-2024-6932	A vulnerability was found in ClassCMS 4.5. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/?action=home&do=shop:index&keyword=&kind=all. The manipulation of the argument order 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-271987.	3.5	More Details
CVE-2024-41663	Canarytokens help track activity and actions on a network. A Cross-Site Scripting vulnerability was identified in the "Cloned Website" Canarytoken, whereby the Canarytoken's creator can attack themselves. The creator of a slow-redirect Canarytoken can insert Javascript into the destination URL of their slow redirect token. When the creator later browses the management page for their own Canarytoken, the Javascript executes. This is a self-XSS. An attacker could create a Canarytoken with this self-XSS, and send the management link to a victim. When they click on it, the Javascript would execute. However, no sensitive information (ex. session information) will be disclosed to the malicious actor. This issue is now patched on Canarytokens.org. Users of self-hosted Canarytokens installations can update by pulling the latest Docker image, or any Docker image after `sha-097d91a`.	3.5	More Details
CVE-2024-6954	A vulnerability was found in SourceCodester Record Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file sort1.php. The manipulation of the argument position 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-272077 was assigned to this vulnerability.	3.5	More Details
CVE-2024-41829	In JetBrains TeamCity before 2024.07 an OAuth code for JetBrains Space could be stolen via Space Application connection	3.5	More Details
CVE-2024-38870	Zohocorp ManageEngine OpManager, OpManager Plus, OpManager MSP and OpManager Enterprise Edition versions before 128104, from 128151 before 128238, from 128247 before 128250 are vulnerable to Stored XSS vulnerability in reports module.	3.5	More Details
CVE-2024-6955	A vulnerability was found in SourceCodester Record Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file sort2.php. The manipulation of the argument qualification 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-272076.	3.5	More Details
CVE-2024-6939	A vulnerability was found in Xinhu RockOA 2.6.3 and classified as problematic. Affected by this issue is the function okla of the file /webmain/public/upload/tpl_upload.html. The manipulation of the argument callback leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-271994 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6907	A vulnerability was found in SourceCodester Record Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file sort.php. The manipulation of the argument sort 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-271932.	3.5	More Details
CVE-2024-6941	A vulnerability, which was classified as problematic, has been found in ThinkSAAS 3.7.0. This issue affects some unknown processing of the file app/system/action/do.php. The manipulation of the argument site_title/site_subtitle/site_key/site_desc/site_url/site_email/site_icp 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-272063.	3.5	More Details
CVE-2024-6942	A vulnerability, which was classified as problematic, was found in ThinkSAAS 3.7.0. Affected is an unknown function of the file app/system/action/anti.php of the component Admin Panel Security Center. The manipulation of the argument ip/email/phone 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-272064.	3.5	More Details
CVE-2024-6938	A vulnerability has been found in SiYuan 3.1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file PDF.js of the component PDF Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-271993 was assigned to this vulnerability.	3.5	More Details
CVE-2024-41826	In JetBrains TeamCity before 2024.07 stored XSS was possible on Show Connection page	3.5	More Details
CVE-2024-32152	A blocklist bypass vulnerability exists in the LaTeX functionality of Ankitects Anki 24.04. A specially crafted malicious flashcard can lead to an arbitrary file creation at a fixed path. An attacker can share a malicious flashcard to trigger this vulnerability.	3.1	More Details
CVE-2023-42010	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.2.5 and 6.2.0.0 through 6.2.0.2 could disclose sensitive information in the HTTP response using man in the middle techniques. IBM X-Force ID: 265507.	3.1	More Details
CVE-2024-6595	An issue was discovered in GitLab CE/EE affecting all versions starting from 11.8 prior to 16.11.6, starting from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2 where it was possible to upload an NPM package with conflicting package data.	3.0	More Details
CVE-2024-40640	vodozemac is an open source implementation of Olm and Megolm in pure Rust. Versions before 0.7.0 of vodozemac use a non-constant time base64 implementation for importing key material for Megolm group sessions and `PkDecryption` Ed25519 secret keys. This flaw might allow an attacker to infer some information about the secret key material through a side-channel attack. The use of a non-constant time base64 implementation might allow an attacker to observe timing variations in the encoding and decoding operations of the secret key material. This could potentially provide insights into the underlying secret key material. The impact of this vulnerability is considered low because exploiting the attacker is required to have access to high precision timing measurements, as well as repeated access to the base64 encoding or decoding processes. Additionally, the estimated leakage amount is bounded and low according to the referenced paper. This has been patched in commit 734b6c6948d4b2bdee3dd8b4efa591d93a61d272 which has been included in release version 0.7.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6694	The WP Mail SMTP plugin for WordPress is vulnerable to information exposure in all versions up to, and including, 4.0.1. This is due to plugin providing the SMTP password in the SMTP Password field when viewing the settings. This makes it possible for authenticated attackers, with administrative-level access and above, to view the SMTP password for the supplied server. Although this would not be useful for attackers in most cases, if an administrator account becomes compromised this could be useful information to an attacker in a limited environment.	2.7	More Details
CVE-2024-6936	A vulnerability, which was classified as problematic, has been found in formtools.org Form Tools 3.1.1. This issue affects some unknown processing of the file /admin/settings/index.php?page=accounts of the component Setting Handler. The manipulation of the argument Page Theme leads to code 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-271991. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.7	More Details
CVE-2024-6937	A vulnerability, which was classified as problematic, was found in formtools.org Form Tools 3.1.1. Affected is the function curl_exec of the file /admin/forms/option_lists/edit.php of the component Import Option List. The manipulation of the argument url leads to file inclusion. 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-271992. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.7	More Details
CVE-2024-41828	In JetBrains TeamCity before 2024.07 comparison of authorization tokens took non-constant time	2.6	More Details
CVE-2024-6807	A vulnerability was found in SourceCodester Student Study Center Desk Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /sscdms/classes/Users.php?f=save of the component HTTP POST Request Handler. The manipulation of the argument firstname/middlename/lastname/username leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2024-6934	A vulnerability classified as problematic has been found in formtools.org Form Tools 3.1.1. This affects an unknown part of the file /admin/forms/add/step2.php?submission_type=direct. The manipulation of the argument Form URL 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-271989 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2024-6935	A vulnerability classified as problematic was found in formtools.org Form Tools 3.1.1. This vulnerability affects unknown code of the file /admin/clients/ of the component User Settings Page. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-271990 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2024-40420	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2024-36694. Reason: This record is a duplicate of CVE-2024-36694. Notes: All CVE users should reference CVE-2024-36694 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0006	Information exposure in the logging system in Yugabyte Platform allows local attackers with access to application logs to obtain database user credentials in log files, potentially leading to unauthorized database access.	N/A	More Details
CVE-2024-24970	Potential vulnerabilities have been identified in the HP Display Control software component within the HP Application Enabling Software Driver which might allow escalation of privilege.	N/A	More Details
CVE-2024-6908	Improper privilege management in Yugabyte Platform allows authenticated admin users to escalate privileges to SuperAdmin via a crafted PUT HTTP request, potentially leading to unauthorized access to sensitive system functions and data.	N/A	More Details
CVE-2024-6895	Insufficient authentication in user account management in Yugabyte Platform allows local network attackers with a compromised user session to change critical security information without re-authentication. An attacker with user session and access to application can modify settings such as password and email without being prompted for the current password, enabling account takeover.	N/A	More Details
CVE-2024-27489	An issue in the DelFile() function of WMCMS v4.4 allows attackers to delete arbitrary files via a crafted POST request.	N/A	More Details
CVE-2024-41661	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-50094. Reason: This candidate is a duplicate of CVE-2023-50094. Notes: All CVE users should reference CVE-2023-50094 instead of this candidate.	N/A	More Details
CVE-2023-4976	A flaw exists in Purity//FB whereby a local account is permitted to authenticate to the management interface using an unintended method that allows an attacker to gain privileged access to the array.	N/A	More Details
CVE-2024-37380	A misconfiguration on UniFi U6+ Access Point could cause an incorrect VLAN traffic forwarding to APs meshed to UniFi U6+ Access Point. Affected Products: UniFi U6+ Access Point (Version 6.6.65 and earlier) Mitigation: Update your UniFi U6+ Access Point to Version 6.6.74 or later.	N/A	More Details
CVE-2024-40639	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2024-6281	A path traversal vulnerability exists in the `apply_settings` function of parisneo/lollms versions prior to 9.5.1. The `sanitize_path` function does not adequately secure the `discussion_db_name` parameter, allowing attackers to manipulate the path and potentially write to important system folders.	N/A	More Details
CVE-2024-7014	EvilVideo vulnerability allows sending malicious apps disguised as videos in Telegram for Android application affecting versions 10.14.4 and older.	N/A	More Details
CVE-2024-40430	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-2024-39152	Rejected reason: DO NOT USE THIS CVE RECORD. Consult IDs: CVE-2024-6655. Reason: This record is a reservation duplicate of CVE-2024-6655. Notes: All CVE users should reference CVE-2024-6655 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34013	Local privilege escalation due to OS command injection vulnerability. The following products are affected: Acronis True Image (macOS) before build 41396.	N/A	More Details
CVE-2024-6765	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details