SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 09 October 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-2024-45519	The postjournal service in Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1 sometimes allows unauthenticated users to execute commands.	10.0	More Details
CVE-2024-47553	A vulnerability has been identified in Siemens SINEC Security Monitor (All versions < V4.9.0). The affected application does not properly validate user input to the ```ssmctl-client``` command. This could allow an authenticated, lowly privileged remote attacker to execute arbitrary code with root privileges on the underlying OS.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20432	A vulnerability in the REST API and web UI of Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an authenticated, low-privileged, remote attacker to perform a command injection attack against an affected device. This vulnerability is due to improper user authorization and insufficient validation of command arguments. An attacker could exploit this vulnerability by submitting crafted commands to an affected REST API endpoint or through the web UI. A successful exploit could allow the attacker to execute arbitrary commands on the CLI of a Cisco NDFC-managed device with network-admin privileges. Note: This vulnerability does not affect Cisco NDFC when it is configured for storage area network (SAN) controller deployment.	9.9	More Details
CVE-2024-45874	A DLL hijacking vulnerability in VegaBird Vooki 5.2.9 allows attackers to execute arbitrary code / maintain persistence via placing a crafted DLL file in the same directory as Vooki.exe.	9.8	More Details
CVE-2024-20101	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998901; Issue ID: MSV-1602.	9.8	More Details
CVE-2024-20103	In wlan firmware, there is a possible out of bounds write due to improper input validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09001358; Issue ID: MSV-1599.	9.8	More Details
CVE-2024-33066	Memory corruption while redirecting log file to any file location with any file name.	9.8	More Details
CVE-2024-9574	SQL injection vulnerability in SOPlanning <1.45, via /soplanning/www/user_groupes.php in the by parameter, which could allow a remote user to submit a specially crafted query, allowing an attacker to retrieve all the information stored in the DB.	9.8	More Details
CVE-2024-46446	Mecha CMS 3.0.0 is vulnerable to Directory Traversal. An attacker can construct cookies and URIs that bypass user identity checks. Parameters can then be passed through the POST method, resulting in the Deletion of Arbitrary Files or Website Takeover.	9.8	More Details
CVE-2024-46076	RuoYi v4.7.9 and before has a security flaw that allows escaping from comments within the code generation feature, enabling the injection of malicious code.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45873	A DLL hijacking vulnerability in VegaBird Yaazhini 2.0.2 allows attackers to execute arbitrary code / maintain persistence via placing a crafted DLL file in the same directory as Yaazhini.exe.	9.8	More Details
CVE-2024-45186	FileSender before 2.49 allows server-side template injection (SSTI) for retrieving credentials.	9.8	More Details
CVE-2024-41798	A vulnerability has been identified in SENTRON 7KM PAC3200 (All versions). Affected devices only provide a 4-digit PIN to protect from administrative access via Modbus TCP interface. Attackers with access to the Modbus TCP interface could easily bypass this protection by brute-force attacks or by sniffing the Modbus clear text communication.	9.8	More Details
CVE-2024-45252	Elsight – CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	9.8	More Details
CVE-2024-8911	The LatePoint plugin for WordPress is vulnerable to Arbitrary User Password Change via SQL Injection in versions up to, and including, 5.0.11. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to change user passwords and potentially take over administrator accounts. Note that changing a WordPress user's password is only possible if the "Use WordPress users as customers" setting is enabled, which is disabled by default. Without this setting enabled, only the passwords of plugin customers, which are stored and managed in a separate database table, can be modified.	9.8	More Details
CVE-2024-8943	The LatePoint plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 5.0.12. This is due to insufficient verification on the user being supplied during the booking customer step. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the user id. Note that logging in as a WordPress user is only possible if the "Use WordPress users as customers" setting is enabled, which is disabled by default. The vulnerability is partially patched in version 5.0.12 and fully patched in version 5.0.13.	9.8	More Details
CVE-2024-8884	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists that could cause exposure of credentials when attacker has access to application on network over http	9.8	More Details
CVE-2024-3057	A flaw exists whereby a user can make a specific call to a FlashArray endpoint allowing privilege escalation.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44349	A SQL injection vulnerability in login portal in AnteeoWMS before v4.7.34 allows unauthenticated attackers to execute arbitrary SQL commands via the username parameter and disclosure of some data in the underlying DB.	9.8	More Details
CVE-2024-45918	Fujian Kelixin Communication Command and Dispatch Platform <=7.6.6.4391 is vulnerable to SQL Injection via /client/get_gis_fence.php.	9.8	More Details
CVE-2024-20100	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998449; Issue ID: MSV-1603.	9.8	More Details
CVE-2024-45251	Elsight – CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	9.8	More Details
CVE-2024-41925	The web service for ONS-S8 - Spectra Aggregation Switch includes functions which do not properly validate user input, allowing an attacker to traverse directories, bypass authentication, and execute remote code.	9.8	More Details
CVE-2024-41593	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to execute arbitrary code via the function ft_payload_dns(), because a byte sign-extension operation occurs for the length argument of a _memcpy call, leading to a heap-based Buffer Overflow.	9.8	More Details
CVE-2024-44097	According to the researcher: "The TLS connections are encrypted against tampering or eavesdropping. However, the application does not validate the server certificate properly while initializing the TLS connection. This allows for a network attacker to intercept the connection and read the data. The attacker could the either send the client a malicious response, or forward the (possibly modified) data to the real server."	9.8	More Details
CVE-2024-24116	An issue in Ruijie RG-NBS2009G-P RGOS v.10.4(1)P2 Release(9736) allows a remote attacker to gain privileges via the system/config_menu.htm.	9.8	More Details
CVE-2024-9441	The Linear eMerge e3-Series through version 1.00-07 is vulnerable to an OS command injection vulnerability. A remote and unauthenticated attacker can execute arbitrary OS commands via the login_id parameter when invoking the forgot_password functionality over HTTP.	9.8	More Details
CVE-2024-24117	Insecure Permissions vulnerability in Ruijie RG-NBS2009G-P RGOS v.10.4(1)P2 Release (9736) allows a remote attacker to gain privileges via the login check state component.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7824	Access of Resource Using Incompatible Type ('Type Confusion') vulnerability in Webroot SecureAnywhere - Web Shield on Windows, ARM, 64 bit, 32 bit (wrUrl.Dll modules) allows Functionality Misuse.This issue affects SecureAnywhere - Web Shield: before 2.1.2.3.	9.8	More Details
CVE-2024-7825	Access of Resource Using Incompatible Type ('Type Confusion') vulnerability in Webroot SecureAnywhere - Web Shield on Windows, ARM, 64 bit, 32 bit (wrUrl.Dll modules) allows Functionality Misuse.This issue affects SecureAnywhere - Web Shield: before 2.1.2.3.	9.8	More Details
CVE-2024-7826	Improper Check for Unusual or Exceptional Conditions vulnerability in Webroot SecureAnywhere - Web Shield on Windows, ARM, 64 bit, 32 bit (wrURL.Dll modules) allows Functionality Misuse.This issue affects SecureAnywhere - Web Shield: before 2.1.2.3.	9.8	More Details
CVE-2024-43468	Microsoft Configuration Manager Remote Code Execution Vulnerability	9.8	More Details
CVE-2024-43699	Delta Electronics DIAEnergie is vulnerable to an SQL injection in the script AM_RegReport.aspx. An unauthenticated attacker may be able to exploit this issue to obtain records contained in the targeted product.	9.8	More Details
CVE-2024-47656	This vulnerability exists in Shilpi Client Dashboard due to missing restrictions for incorrect login attempts on its API based login. A remote attacker could exploit this vulnerability by conducting a brute force attack on password, which could lead to gain unauthorized access to other user accounts.	9.8	More Details
CVE-2023-26770	TaskCafe 0.3.2 lacks validation in the Cookie value. Any unauthenticated attacker who knows a registered UserID can change the password of that user.	9.8	More Details
CVE-2024-43685	Improper Authentication vulnerability in Microchip TimeProvider 4100 (login modules) allows Session Hijacking.This issue affects TimeProvider 4100: from 1.0 before 2.4.7.	9.8	More Details
CVE-2024-47849	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in The Wikimedia Foundation Mediawiki - Cargo allows SQL Injection.This issue affects Mediawiki - Cargo: from 3.6.X before 3.6.1.	9.8	More Details
CVE-2024-45249	Cavok – CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44014	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Vmaxstudio Vmax Project Manager allows PHP Local File Inclusion, Code Injection.This issue affects Vmax Project Manager: from n/a through 1.0.	9.6	More Details
CVE-2024-47350	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in YITH YITH WooCommerce Ajax Search allows SQL Injection.This issue affects YITH WooCommerce Ajax Search: from n/a through 2.8.0.	9.3	More Details
CVE-2024-45367	The web server for ONS-S8 - Spectra Aggregation Switch includes an incomplete authentication process, which can lead to an attacker authenticating without a password.	9.1	More Details
CVE-2024-35293	An unauthenticated remote attacker may use a missing authentication for critical function vulnerability to reboot or erase the affected devices resulting in data loss and/or a DoS.	9.1	More Details
CVE-2024-38124	Windows Netlogon Elevation of Privilege Vulnerability	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-9603	Type Confusion in V8 in Google Chrome prior to 129.0.6668.100 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-43592	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-47655	This vulnerability exists in the Shilpi Client Dashboard due to improper validation of files being uploaded other than the specified extension. An authenticated remote attacker could exploit this vulnerability by uploading malicious file, which could lead to remote code execution on targeted application.	8.8	More Details
CVE-2024-43599	Remote Desktop Client Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43564	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-9556	A vulnerability, which was classified as critical, was found in D-Link DIR-605L 2.13B01 BETA. This affects the function formSetEnableWizard of the file /goform/formSetEnableWizard. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9555	A vulnerability, which was classified as critical, has been found in D-Link DIR-605L 2.13B01 BETA. Affected by this issue is the function formSetEasy_Wizard of the file /goform/formSetEasy_Wizard. The manipulation of the argument curTime leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-42417	Delta Electronics DIAEnergie is vulnerable to an SQL injection in the script Handler_CFG.ashx. An authenticated attacker may be able to exploit this issue to cause delay in the targeted product.	8.8	More Details
CVE-2024-41589	DrayTek Vigor310 devices through 4.3.2.6 use unencrypted HTTP for authentication requests.	8.8	More Details
CVE-2024-9558	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This issue affects the function formSetWanPPTP of the file /goform/formSetWanPPTP. The manipulation of the argument webpage leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-43607	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-43608	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-47562	A vulnerability has been identified in Siemens SINEC Security Monitor (All versions < V4.9.0). The affected application does not properly neutralize special elements in user input to the ```ssmctl-client``` command. This could allow an authenticated, lowly privileged local attacker to execute privileged commands in the underlying OS.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43611	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-9313	Authd PAM module before version 0.3.5 can allow broker-managed users to impersonate any other user managed by the same broker and perform any PAM operation with it, including authenticating as them.	8.8	More Details
CVE-2024-43549	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-28888	A use-after-free vulnerability exists in the way Foxit Reade 2024.1.0.23997 handles a checkbox field object. A specially crafted Javascript code inside a malicious PDF document can trigger this vulnerability, which can lead to memory corruption and result in arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.	8.8	More Details
CVE-2024-9533	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This issue affects the function formDeviceReboot of the file /goform/formDeviceReboot. The manipulation of the argument next_page leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-7612	Insecure permissions in Ivanti EPMM before 12.1.0.4 allow a local authenticated attacker to modify sensitive application components.	8.8	More Details
CVE-2024-46626	OS4ED openSIS-Classic v9.1 was discovered to contain a SQL injection vulnerability via a crafted payload.	8.8	More Details
CVE-2024-9553	A vulnerability classified as critical has been found in D-Link DIR-605L 2.13B01 BETA. This affects the function formdumpeasysetup of the file /goform/formdumpeasysetup. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9534	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. Affected is the function formEasySetPassword of the file /goform/formEasySetPassword. The manipulation of the argument curTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9535	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been declared as critical. Affected by this vulnerability is the function formEasySetupWWConfig of the file /goform/formEasySetupWWConfig. The manipulation of the argument curTime leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-43593	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-9514	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been declared as critical. This vulnerability affects the function formSetDomainFilter of the file /goform/formSetDomainFilter. The manipulation of the argument curTime leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-38179	Azure Stack Hyperconverged Infrastructure (HCI) Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-9515	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. This affects the function formSetQoS of the file /goform/formSetQoS. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9561	A vulnerability classified as critical has been found in D-Link DIR-605L 2.13B01 BETA. This affects the function formSetWAN_Wizard51/formSetWAN_Wizard52. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9532	A vulnerability has been found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This vulnerability affects the function formAdvanceSetup of the file /goform/formAdvanceSetup. The manipulation of the argument webpage leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9562	A vulnerability classified as critical was found in D-Link DIR-605L 2.13B01 BETA. This vulnerability affects the function formSetWizard1/formSetWizard2. The manipulation of the argument curTime leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9563	A vulnerability, which was classified as critical, has been found in D-Link DIR-605L 2.13B01 BETA. This issue affects the function formWlanSetup_Wizard of the file /goform/formWlanSetup_Wizard. The manipulation of the argument webpage leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9564	A vulnerability, which was classified as critical, was found in D-Link DIR-605L 2.13B01 BETA. Affected is the function formWlanWizardSetup of the file /goform/formWlanWizardSetup. The manipulation of the argument webpage leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9565	A vulnerability has been found in D-Link DIR-605L 2.13B01 BETA and classified as critical. Affected by this vulnerability is the function formSetPassword of the file /goform/formSetPassword. The manipulation of the argument curTime leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-47846	Cross-Site Request Forgery (CSRF) vulnerability in The Wikimedia Foundation Mediawiki - Cargo allows Cross Site Request Forgery.This issue affects Mediawiki - Cargo: from 3.6.X before 3.6.1.	8.8	More Details
CVE-2024-37869	File Upload vulnerability in Itsourcecode Online Discussion Forum Project v.1.0 allows a remote attacker to execute arbitrary code via the "poster.php" file, and the uploaded file was received using the "$- FILES" variable	8.8	More Details
CVE-2024-37868	File Upload vulnerability in Itsourcecode Online Discussion Forum Project v.1.0 allows a remote attacker to execute arbitrary code via the "sendreply.php" file, and the uploaded file was received using the "$-FILES" variable.	8.8	More Details
CVE-2024-9054	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Microchip TimeProvider 4100 (Configuration modules) allows Command Injection.This issue affects TimeProvider 4100: from 1.0 before 2.4.7.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43589	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-43684	Cross-Site Request Forgery (CSRF) vulnerability in Microchip TimeProvider 4100 allows Cross Site Request Forgery, Cross-Site Scripting (XSS).This issue affects TimeProvider 4100: from 1.0.	8.8	More Details
CVE-2024-41512	A SQL Injection vulnerability in "ccHandler.aspx" in all versions of CADClick v.1.11.0 and before allows remote attackers to execute arbitrary SQL commands via the "bomid" parameter.	8.8	More Details
CVE-2024-9566	A vulnerability classified as critical was found in D-Link DIR-619L B1 2.06. This vulnerability affects the function formDeviceReboot of the file /goform/formDeviceReboot. The manipulation of the argument next_page leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9567	A vulnerability, which was classified as critical, has been found in D-Link DIR-619L B1 2.06. This issue affects the function formAdvFirewall of the file /goform/formAdvFirewall. The manipulation of the argument curTime leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9557	A vulnerability has been found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This vulnerability affects the function formSetWanPPPoE of the file /goform/formSetWanPPPoE. The manipulation of the argument webpage leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9568	A vulnerability, which was classified as critical, was found in D-Link DIR-619L B1 2.06. Affected is the function formAdvNetwork of the file /goform/formAdvNetwork. The manipulation of the argument curTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9569	A vulnerability has been found in D-Link DIR-619L B1 2.06 and classified as critical. Affected by this vulnerability is the function formEasySetPassword of the file /goform/formEasySetPassword. The manipulation of the argument curTime leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46041	IoT Haat Smart Plug IH-IN-16A-S v5.16.1 is vulnerable to Authentication Bypass by Capture-replay.	8.8	More Details
CVE-2024-9570	A vulnerability was found in D-Link DIR-619L B1 2.06 and classified as critical. Affected by this issue is the function formEasySetTimezone of the file /goform/formEasySetTimezone. The manipulation of the argument curTime leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-27458	A potential security vulnerability has been identified in the HP Hotkey Support software, which might allow local escalation of privilege. HP is releasing mitigation for the potential vulnerability. Customers using HP Programmable Key are recommended to update HP Hotkey Support.	8.8	More Details
CVE-2024-9552	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been rated as critical. Affected by this issue is the function formSetWanNonLogin of the file /goform/formSetWanNonLogin. The manipulation of the argument webpage leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9559	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. Affected is the function formWlanSetup of the file /goform/formWlanSetup. The manipulation of the argument webpage leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-38212	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-9549	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This issue affects the function formEasySetupWizard/formEasySetupWizard2 of the file /goform/formEasySetupWizard. The manipulation of the argument curTime leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-8885	A local privilege escalation vulnerability in Sophos Intercept X for Windows with Central Device Encryption 2024.2.0 and older allows writing of arbitrary files.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9550	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. Affected is the function formLogDnsquery of the file /goform/formLogDnsquery. The manipulation of the argument curTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-20393	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin.	8.8	More Details
CVE-2024-43518	Windows Telephony Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-43453	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-43519	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-38265	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-43517	Microsoft ActiveX Data Objects Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-43488	Missing authentication for critical function in Visual Studio Code extension for Arduino allows an unauthenticated attacker to perform remote code execution through network attack vector.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20449	A vulnerability in Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an authenticated, remote attacker with low privileges to execute arbitrary code on an affected device. This vulnerability is due to improper path validation. An attacker could exploit this vulnerability by using the Secure Copy Protocol (SCP) to upload malicious code to an affected device using path traversal techniques. A successful exploit could allow the attacker to execute arbitrary code in a specific container with the privileges of root.	8.8	More Details
CVE-2024-9551	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been declared as critical. Affected by this vulnerability is the function formSetWanL2TP of the file /goform/formSetWanL2TP. The manipulation of the argument webpage leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-7855	The WP Hotel Booking plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the update_review() function in all versions up to, and including, 2.1.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2024-43532	Remote Registry Service Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-43533	Remote Desktop Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-9602	Type Confusion in V8 in Google Chrome prior to 129.0.6668.100 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-43591	Azure Command Line Integration (CLI) Elevation of Privilege Vulnerability	8.7	More Details
CVE-2024-7558	JUJU_CONTEXT_ID is a predictable authentication secret. On a Juju machine (non-Kubernetes) or Juju charm container (on Kubernetes), an unprivileged user in the same network namespace can connect to an abstract domain socket and guess the JUJU_CONTEXT_ID value. This gives the unprivileged user access to the same information and tools as the Juju charm.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20498	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.	8.6	More Details
CVE-2024-20499	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.	8.6	More Details
CVE-2024-20501	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52952	A vulnerability has been identified in HiMed Cockpit 12 pro (J31032-K2017-H259) (All versions >= V11.5.1 < V11.6.2), HiMed Cockpit 14 pro+ (J31032-K2017-H435) (All versions >= V11.5.1 < V11.6.2), HiMed Cockpit 18 pro (J31032-K2017-H260) (All versions >= V11.5.1 < V11.6.2), HiMed Cockpit 18 pro+ (J31032-K2017-H436) (All versions >= V11.5.1 < V11.6.2). The Kiosk Mode of the affected devices contains a restricted desktop environment escape vulnerability. This could allow an unauthenticated local attacker to escape the restricted environment and gain access to the underlying operating system.	8.5	More Details
CVE-2024-46278	Teedy 1.11 is vulnerable to Cross Site Scripting (XSS) via the management console.	8.4	More Details
CVE-2024-36474	An integer overflow vulnerability exists in the Compound Document Binary File format parser of the GNOME Project G Structured File Library (libgsf) version v1.14.52. A specially crafted file can result in an integer overflow when processing the directory from the file that allows for an out-of-bounds index to be used when reading and writing to an array. This can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.4	More Details
CVE-2024-43497	DeepSpeed Remote Code Execution Vulnerability	8.4	More Details
CVE-2024-38399	Memory corruption while processing user packets to generate page faults.	8.4	More Details
CVE-2024-33065	Memory corruption while taking snapshot when an offset variable is set by camera driver.	8.4	More Details
CVE-2024-8215	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Payara Platform Payara Server (Admin Console modules) allows Remote Code Inclusion.This issue affects Payara Server: from 5.20.0 before 5.68.0, from 6.0.0 before 6.19.0, from 6.2022.1 before 6.2024.10, from 4.1.2.191.1 before 4.1.2.191.51.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42415	An integer overflow vulnerability exists in the Compound Document Binary File format parser of v1.14.52 of the GNOME Project G Structured File Library (libgsf). A specially crafted file can result in an integer overflow that allows for a heap-based buffer overflow when processing the sector allocation table. This can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.4	More Details
CVE-2024-47555	Missing Authentication - User & System Configuration	8.3	More Details
CVE-2024-47557	Pre-Auth RCE via Path Traversal	8.3	More Details
CVE-2024-47556	Pre-Auth RCE via Path Traversal	8.3	More Details
CVE-2024-43574	Microsoft Speech Application Programming Interface (SAPI) Remote Code Execution Vulnerability	8.3	More Details
CVE-2024-47845	Improper Encoding or Escaping of Output vulnerability in The Wikimedia Foundation Mediawiki - CSS Extension allows Code Injection.This issue affects Mediawiki - CSS Extension: from 1.39.X before 1.39.9, from 1.41.X before 1.41.3, from 1.42.X before 1.42.2.	8.2	More Details
CVE-2024-45051	Discourse is an open source platform for community discussion. A maliciously crafted email address could allow an attacker to bypass domain-based restrictions and gain access to private sites, categories and/or groups. This issue has been patched in the latest stable, beta and tests-passed version of Discourse. All users area are advised to upgrade. There are no known workarounds for this vulnerability.	8.2	More Details
CVE-2023-37822	The Eufy Homebase 2 before firmware version 3.3.4.1h creates a dedicated wireless network for its ecosystem, which serves as a proxy to the end user's primary network. The WPA2-PSK generation of this dedicated network is flawed and solely based on the serial number. Due to the flawed generation process, the WPA2-PSK can be brute forced offline within seconds. This vulnerability allows an attacker in proximity to the dedicated wireless network to gain unauthorized access to the end user's primary network. The only requirement of the attack is proximity to the dedicated wireless network.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33064	Information disclosure while parsing the multiple MBSSID IEs from the beacon.	8.2	More Details
CVE-2024-47773	Discourse is an open source platform for community discussion. An attacker can make several XHR requests until the cache is poisoned with a response without any preloaded data. This issue only affects anonymous visitors of the site. This problem has been patched in the latest version of Discourse. Users are advised to upgrade. Users unable to upgrade should disable anonymous cache by setting the `DISCOURSE_DISABLE_ANON_CACHE` environment variable to a non-empty value.	8.2	More Details
CVE-2024-46539	Insecure permissions in the Bluetooth Low Energy (BLE) component of Fire-Boltt Artillery Smart Watch NJ-R6E-10.3 allow attackers to cause a Denial of Service (DoS).	8.2	More Details
CVE-2024-33073	Information disclosure while parsing the BSS parameter change count or MLD capabilities fields of the ML IE.	8.2	More Details
CVE-2024-47807	Jenkins OpenId Connect Authentication Plugin 4.354.v321ce67a_1de8 and earlier does not check the `iss` (Issuer) claim of an ID Token, allowing attackers to subvert the authentication flow, potentially gaining administrator access to Jenkins.	8.1	More Details
CVE-2024-8926	In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, when using a certain non-standard configurations of Windows codepages, the fixes for CVE-2024-4577 https://github.com/advisories/GHSA-vxpp-6299-mxw3 may still be bypassed and the same command injection related to Windows "Best Fit" codepage behavior can be achieved. This may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.	8.1	More Details
CVE-2024-47323	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ex-Themes WP Timeline – Vertical and Horizontal timeline plugin allows PHP Local File Inclusion.This issue affects WP Timeline – Vertical and Horizontal timeline plugin: from n/a through 3.6.7.	8.1	More Details
CVE-2024-47806	Jenkins OpenId Connect Authentication Plugin 4.354.v321ce67a_1de8 and earlier does not check the `aud` (Audience) claim of an ID Token, allowing attackers to subvert the authentication flow, potentially gaining administrator access to Jenkins.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47652	This vulnerability exists in Shilpi Client Dashboard due to implementation of inadequate authentication mechanism in the login module wherein access to any users account is granted with just their corresponding mobile number. A remote attacker could exploit this vulnerability by providing mobile number of targeted user, to obtain complete access to the targeted user account.	8.1	More Details
CVE-2024-44068	An issue was discovered in the m2m scaler driver in Samsung Mobile Processor and Wearable Processor Exynos 9820, 9825, 980, 990, 850,and W920. A Use-After-Free in the mobile processor leads to privilege escalation.	8.1	More Details
CVE-2024-47183	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. If the Parse Server option allowCustomObjectId: true is set, an attacker that is allowed to create a new user can set a custom object ID for that new user that exploits the vulnerability and acquires privileges of a specific role. This vulnerability is fixed in 6.5.9 and 7.3.0.	8.1	More Details
CVE-2024-47768	Lif Authentication Server is a server used by Lif to do various tasks regarding Lif accounts. This vulnerability has to do with the account recovery system where there does not appear to be a check to make sure the user has been sent the recovery email and entered the correct code. If the attacker knew the email of the target, they could supply the email and immediately prompt the server to update the password without ever needing the code. This issue has been patched in version 1.7.3.	8.1	More Details
CVE-2024-44023	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ABCApp Creator allows PHP Local File Inclusion.This issue affects ABCApp Creator: from n/a through 1.1.2.	8.1	More Details
CVE-2024-41290	FlatPress CMS v1.3.1 1.3 was discovered to use insecure methods to store authentication data via the cookie's component.	8.1	More Details
CVE-2024-43582	Remote Desktop Protocol Server Remote Code Execution Vulnerability	8.1	More Details
CVE-2024-38229	.NET and Visual Studio Remote Code Execution Vulnerability	8.1	More Details
CVE-2024-47319	Unrestricted Upload of File with Dangerous Type vulnerability in Bit Apps Bit Form – Contact Form Plugin allows Code Injection.This issue affects Bit Form – Contact Form Plugin: from n/a through 2.13.10.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46658	Syrotech SY-GOPON-8OLT-L3 v1.6.0_240629 was discovered to contain an authenticated command injection vulnerability.	8.0	More Details
CVE-2024-41596	Buffer Overflow vulnerabilities exist in DrayTek Vigor310 devices through 4.3.2.6 (in the Vigor management UI) because of improper retrieval and handling of the CGI form parameters.	8.0	More Details
CVE-2024-41595	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to change settings or cause a denial of service via .cgi pages because of missing bounds checks on read and write operations.	8.0	More Details
CVE-2024-41592	DrayTek Vigor3910 devices through 4.3.2.6 have a stack-based overflow when processing query string parameters because GetCGI mishandles extraneous ampersand characters and long key-value pairs.	8.0	More Details
CVE-2024-41590	Several CGI endpoints are vulnerable to buffer overflows, by authenticated users, because of missing bounds checking on parameters passed through POST requests to the strcpy function on DrayTek Vigor310 devices through 4.3.2.6.	8.0	More Details
CVE-2024-41588	The CGI endpoints v2x00.cgi and cgiwcg.cgi of DrayTek Vigor3910 devices through 4.3.2.6 are vulnerable to buffer overflows, by authenticated users, because of missing bounds checking on parameters passed through POST requests to the strncpy function.	8.0	More Details
CVE-2024-46486	TP-LINK TL-WDR5620 v2.3 was discovered to contain a remote code execution (RCE) vulnerability via the httpProcDataSrv function.	8.0	More Details
CVE-2024-41586	A stack-based Buffer Overflow vulnerability in DrayTek Vigor310 devices through 4.3.2.6 allows a remote attacker to execute arbitrary code via a long query string to the cgi-bin/ipfedr.cgi component.	8.0	More Details
CVE-2024-8733	A potential security vulnerability has been identified in the HP One Agent for certain HP PC products, which might allow for escalation of privilege. HP is releasing software updates to mitigate this potential vulnerability.	8.0	More Details
CVE-2024-45880	A command injection vulnerability exists in Motorola CX2L router v1.0.2 and below. The vulnerability is present in the SetStationSettings function. The system directly invokes the system function to execute commands for setting parameters such as MAC address without proper input filtering. This allows malicious users to inject and execute arbitrary commands.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30092	Windows Hyper-V Remote Code Execution Vulnerability	8.0	More Details
CVE-2024-8038	Vulnerable juju introspection abstract UNIX domain socket. An abstract UNIX domain socket responsible for introspection is available without authentication locally to network namespace users. This enables denial of service attacks.	7.9	More Details
CVE-2024-43504	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-43503	Microsoft SharePoint Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-43505	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-38261	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-43556	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-9167	Under specific circumstances, insecure permissions in Ivanti Velocity License Server before version 5.2 allows a local authenticated attacker to achieve local privilege escalation.	7.8	More Details
CVE-2024-21455	Memory corruption when a compat IOCTL call is followed by another IOCTL call from userspace to a driver.	7.8	More Details
CVE-2024-47134	Out-of-bounds write vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC Programming Software) Version 1.6.14.0 and earlier. Having a user open a specially crafted project file which was saved using Kostac PLC Programming Software Version 1.6.9.0 and earlier may cause a denial-of-service (DoS) condition, arbitrary code execution, and/or information disclosure because the issues exist in parsing of KPP project files.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43560	Microsoft Windows Storage Port Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-20092	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1700.	7.8	More Details
CVE-2024-43563	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-47135	Stack-based buffer overflow vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC Programming Software) Version 1.6.14.0 and earlier. Having a user open a specially crafted project file which was saved using Kostac PLC Programming Software Version 1.6.9.0 and earlier may cause a denial-of-service (DoS) condition, arbitrary code execution, and/or information disclosure because the issues exist in parsing of KPP project files.	7.8	More Details
CVE-2024-43583	Winlogon Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-43572	Microsoft Management Console Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-47136	Out-of-bounds read vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC Programming Software) Version 1.6.14.0 and earlier. Having a user open a specially crafted project file which was saved using Kostac PLC Programming Software Version 1.6.9.0 and earlier may cause a denial-of-service (DoS) condition, arbitrary code execution, and/or information disclosure because the issues exist in parsing of KPP project files.	7.8	More Details
CVE-2024-45469	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43527	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-43551	Windows Storage Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-8422	CWE-416: Use After Free vulnerability exists that could cause arbitrary code execution, denial of service and loss of confidentiality & integrity when application user opens a malicious Zelio Soft 2 project file.	7.8	More Details
CVE-2024-47046	A vulnerability has been identified in Simcenter Femap V2306 (All versions), Simcenter Femap V2401 (All versions), Simcenter Femap V2406 (All versions). The affected application is vulnerable to memory corruption while parsing specially crafted BDF files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-43576	Microsoft Office Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-43528	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-45470	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-23369	Memory corruption when invalid length is provided from HLOS for FRS/UDS request/response buffers.	7.8	More Details
CVE-2024-41981	A vulnerability has been identified in Simcenter Femap V2306 (All versions), Simcenter Femap V2401 (All versions), Simcenter Femap V2406 (All versions). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted BDF files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45468	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-45467	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-45466	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-45465	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45464	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-45471	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-45463	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-45472	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process.	7.8	More Details
CVE-2024-43047	Memory corruption while maintaining memory maps of HLOS memory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45473	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process.	7.8	More Details
CVE-2024-45474	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process.	7.8	More Details
CVE-2024-43509	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-43516	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-45475	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected application is vulnerable to memory corruption while parsing specially crafted WRL files. An attacker could leverage this in conjunction with other vulnerabilities to execute code in the context of the current process.	7.8	More Details
CVE-2024-43590	Visual C++ Redistributable Installer Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41902	A vulnerability has been identified in JT2Go (All versions < V2406.0003). The affected application contains a stack-based buffer overflow vulnerability that could be triggered while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-45245	Diebold Nixdorf – CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	7.8	More Details
CVE-2024-43616	Microsoft Office Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-39755	A privilege escalation vulnerability exists in the node update functionality of Veertu Anka Build 1.42.0. A specially crafted PKG file can lead to execute priviledged operation. An attacker can make an unauthenticated HTTP request to trigger this vulnerability.	7.8	More Details
CVE-2024-43601	Visual Studio Code for Linux Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-43514	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-43501	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-44193	A logic issue was addressed with improved restrictions. This issue is fixed in iTunes 12.13.3 for Windows. A local attacker may be able to elevate their privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45290	PHPSpreadsheet is a pure PHP library for reading and writing spreadsheet files. It's possible for an attacker to construct an XLSX file which links media from external URLs. When opening the XLSX file, PhpSpreadsheet retrieves the image size and type by reading the file contents, if the provided path is a URL. By using specially crafted `php://filter` URLs an attacker can leak the contents of any file or URL. Note that this vulnerability is different from GHSA-w9xv-qf98-ccq4, and resides in a different component. An attacker can access any file on the server, or leak information form arbitrary URLs, potentially exposing sensitive information such as AWS IAM credentials. This issue has been addressed in release versions 1.29.2, 2.1.1, and 2.3.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	7.7	More Details
CVE-2024-37179	SAP BusinessObjects Business Intelligence Platform allows an authenticated user to send a specially crafted request to the Web Intelligence Reporting Server to download any file from the machine hosting the service, causing high impact on confidentiality of the application.	7.7	More Details
CVE-2024-43584	Windows Scripting Engine Security Feature Bypass Vulnerability	7.7	More Details
CVE-2024-47559	Authenticated RCE via Path Traversal	7.6	More Details
CVE-2024-47558	Authenticated RCE via Path Traversal	7.6	More Details
CVE-2024-47335	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Bit Form Bit Form – Contact Form Plugin allows SQL Injection.This issue affects Bit Form – Contact Form Plugin: from n/a through 2.13.11.	7.6	More Details
CVE-2024-47338	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPExpertsio WPExperts Square For GiveWP allows SQL Injection.This issue affects WPExperts Square For GiveWP: from n/a through 1.3.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47782	WikiDiscover is an extension designed for use with a CreateWiki managed farm to display wikis. Special:WikiDiscover is a special page that lists all wikis on the wiki farm. However, the special page does not make any effort to escape the wiki name or description. Therefore, if a wiki sets its name and/or description to an XSS payload, the XSS will execute whenever the wiki is shown on Special:WikiDiscover. This issue has been patched with commit `2ce846dd93` and all users are advised to apply that patch. User unable to upgrade should block access to `Special:WikiDiscover`.	7.6	More Details
CVE-2024-47011	Path Traversal in Ivanti Avalanche before version 6.4.5 allows a remote unauthenticated attacker to leak sensitive information	7.5	More Details
CVE-2024-38129	Windows Kerberos Elevation of Privilege Vulnerability	7.5	More Details
CVE-2024-44011	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WP Ticket Ultra WP Ticket Ultra Help Desk & Support Plugin allows PHP Local File Inclusion.This issue affects WP Ticket Ultra Help Desk & Support Plugin: from n/a through 1.0.5.	7.5	More Details
CVE-2024-44012	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in wpdev33 WP Newsletter Subscription allows PHP Local File Inclusion.This issue affects WP Newsletter Subscription: from n/a through 1.1.	7.5	More Details
CVE-2024-43544	Microsoft Simple Certificate Enrollment Protocol Denial of Service Vulnerability	7.5	More Details
CVE-2024-33069	Transient DOS when transmission of management frame sent by host is not successful and error status is received in the host.	7.5	More Details
CVE-2024-45230	An issue was discovered in Django 5.1 before 5.1.1, 5.0 before 5.0.9, and 4.2 before 4.2.16. The urlize() and urlizetrunc() template filters are subject to a potential denial-of-service attack via very large inputs with a specific sequence of characters.	7.5	More Details
CVE-2024-46078	itsourcecode Sports Management System Project 1.0 is vulnerable to SQL Injection in the function delete_category of the file sports_scheduling/player.php via the argument id.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33070	Transient DOS while parsing ESP IE from beacon/probe response frame.	7.5	More Details
CVE-2024-44013	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Innate Images LLC VR Calendar allows PHP Local File Inclusion.This issue affects VR Calendar: from n/a through 2.4.0.	7.5	More Details
CVE-2024-44015	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Users Control allows PHP Local File Inclusion.This issue affects Users Control: from n/a through 1.0.16.	7.5	More Details
CVE-2024-44016	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Mark Steadman Podiant allows PHP Local File Inclusion.This issue affects Podiant: from n/a through 1.1.	7.5	More Details
CVE-2024-33049	Transient DOS while parsing noninheritance IE of Extension element when length of IE is 2 of beacon frame.	7.5	More Details
CVE-2024-47007	A NULL pointer dereference in WLAvalancheService.exe of Ivanti Avalanche before version 6.4.5 allows a remote unauthenticated attacker to cause a denial of service.	7.5	More Details
CVE-2024-7315	The Migration, Backup, Staging WordPress plugin before 0.9.106 does not use sufficient randomness in the filename that is created when generating a backup, which could be bruteforced by attackers to leak sensitive information about said backups.	7.5	More Details
CVE-2024-38029	Microsoft OpenSSH for Windows Remote Code Execution Vulnerability	7.5	More Details
CVE-2024-25885	An issue in the getcolor function in utils.py of xhtml2pdf v0.2.13 allows attackers to cause a Regular expression Denial of Service (ReDOS) via supplying a crafted string.	7.5	More Details
CVE-2024-43521	Windows Hyper-V Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47841	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in The Wikimedia Foundation Mediawiki - CSS Extension allows Path Traversal.This issue affects Mediawiki - CSS Extension: from 1.42.X before 1.42.2, from 1.41.X before 1.41.3, from 1.39.X before 1.39.9.	7.5	More Details
CVE-2024-43541	Microsoft Simple Certificate Enrollment Protocol Denial of Service Vulnerability	7.5	More Details
CVE-2024-44018	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Istmo Plugins Instant Chat Floating Button for WordPress Websites allows PHP Local File Inclusion.This issue affects Instant Chat Floating Button for WordPress Websites: from n/a through 1.0.5.	7.5	More Details
CVE-2024-20094	In Modem, there is a possible system crash due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00843282; Issue ID: MSV-1535.	7.5	More Details
CVE-2024-43575	Windows Hyper-V Denial of Service Vulnerability	7.5	More Details
CVE-2024-47008	Server-side request forgery in Ivanti Avalanche before version 6.4.5 allows a remote unauthenticated attacker to leak sensitive information.	7.5	More Details
CVE-2024-38262	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	7.5	More Details
CVE-2024-33071	Transient DOS while parsing the MBSSID IE from the beacons when IE length is 0.	7.5	More Details
CVE-2024-8352	The Social Web Suite – Social Media Auto Post, Social Media Auto Publish plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 4.1.11 via the download_log function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	7.5	More Details
CVE-2024-38397	Transient DOS while parsing probe response and assoc response frame.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34666	Out-of-bounds write in parsing h.264 format in a specific mode in librtppayload.so prior to SMR Oct-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability.	7.5	More Details
CVE-2024-47324	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ex-Themes WP Timeline – Vertical and Horizontal timeline plugin allows PHP Local File Inclusion.This issue affects WP Timeline – Vertical and Horizontal timeline plugin: from n/a through 3.6.7.	7.5	More Details
CVE-2024-43567	Windows Hyper-V Denial of Service Vulnerability	7.5	More Details
CVE-2024-43565	Windows Network Address Translation (NAT) Denial of Service Vulnerability	7.5	More Details
CVE-2024-43562	Windows Network Address Translation (NAT) Denial of Service Vulnerability	7.5	More Details
CVE-2024-38149	BranchCache Denial of Service Vulnerability	7.5	More Details
CVE-2024-25590	An attacker can publish a zone containing specific Resource Record Sets. Repeatedly processing and caching results for these sets can lead to a denial of service.	7.5	More Details
CVE-2024-34665	Out-of-bounds write in parsing h.264 format in librtppayload.so prior to SMR Oct-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability.	7.5	More Details
CVE-2024-34667	Out-of-bounds write in parsing h.265 format in librtppayload.so prior to SMR Oct-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability.	7.5	More Details
CVE-2024-33662	Portainer before 2.20.2 improperly uses an encryption algorithm in the AesEncrypt function.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34668	Out-of-bounds write in parsing h.263 format in librtppayload.so prior to SMR Oct-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability.	7.5	More Details
CVE-2024-34669	Out-of-bounds write in parsing h.263+ format in librtppayload.so prior to SMR Oct-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability.	7.5	More Details
CVE-2024-47850	CUPS cups-browsed before 2.5b1 will send an HTTP POST request to an arbitrary destination and port in response to a single IPP UDP packet requesting a printer to be added, a different vulnerability than CVE-2024-47176. (The request is meant to probe the new printer but can be used to create DDoS amplification attacks.)	7.5	More Details
CVE-2024-41163	A directory traversal vulnerability exists in the archive functionality of Veertu Anka Build 1.42.0. A specially crafted HTTP request can lead to a disclosure of sensitive information. An attacker can make an unauthenticated HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2024-41922	A directory traversal vulnerability exists in the log files download functionality of Veertu Anka Build 1.42.0. A specially crafted HTTP request can lead to a disclosure of sensitive information. An attacker can make an unauthenticated HTTP request to trigger this vulnerability.	7.5	More Details
CVE-2024-41594	An issue in DrayTek Vigor310 devices through 4.3.2.6 allows an attacker to obtain sensitive information because the httpd server of the Vigor management UI uses a static string for seeding the PRNG of OpenSSL.	7.5	More Details
CVE-2024-47805	Jenkins Credentials Plugin 1380.va_435002fa_924 and earlier, except 1371.1373.v4eb_fa_b_7161e9, does not redact encrypted values of credentials using the `SecretBytes` type when accessing item `config.xml` via REST API or CLI.	7.5	More Details
CVE-2024-5803	The AVGUI.exe of AVG/Avast Antivirus before versions before 24.1 can allow a local attacker to escalate privileges via an COM hijack in a time-of-check to time-of-use (TOCTOU) when self protection is disabled.	7.5	More Details
CVE-2024-43789	Discourse is an open source platform for community discussion. A user can create a post with many replies, and then attempt to fetch them all at once. This can potentially reduce the availability of a Discourse instance. This problem has been patched in the latest version of Discourse. All users area are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47614	async-graphql is a GraphQL server library implemented in Rust. async-graphql before 7.0.10 does not limit the number of directives for a field. This can lead to Service Disruption, Resource Exhaustion, and User Experience Degradation. This vulnerability is fixed in 7.0.10.	7.5	More Details
CVE-2024-6400	Cleartext Storage of Sensitive Information vulnerability in Finrota Netahsilat allows Retrieve Embedded Sensitive Data.This issue solved in versions 1.21.10, 1.23.01, 1.23.08, 1.23.11 and 1.24.03.	7.5	More Details
CVE-2024-38040	There is a local file inclusion vulnerability in Esri Portal for ArcGIS 11.2. 11.1, 11.0 and 10.9.1 that may allow a remote, unauthenticated attacker to craft a URL that could potentially disclose sensitive configuration information by reading internal files.	7.5	More Details
CVE-2024-43515	Internet Small Computer Systems Interface (iSCSI) Denial of Service Vulnerability	7.5	More Details
CVE-2024-44017	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in MinHyeong Lim MH Board allows PHP Local File Inclusion.This issue affects MH Board: from n/a through 1.3.2.1.	7.5	More Details
CVE-2024-44034	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Martin Greenwood WPSPX allows PHP Local File Inclusion.This issue affects WPSPX: from n/a through 1.0.2.	7.5	More Details
CVE-2024-43506	BranchCache Denial of Service Vulnerability	7.5	More Details
CVE-2024-43545	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability	7.5	More Details
CVE-2024-45248	Multi-DNC – CWE-35: Path Traversal: '.../...//'	7.5	More Details
CVE-2024-47769	IDURAR is open source ERP CRM accounting invoicing software. The vulnerability exists in the corePublicRouter.js file. Using the reference usage here, it is identified that the public endpoint is accessible to an unauthenticated user. The user's input is directly appended to the join statement without additional checks. This allows an attacker to send URL encoded malicious payload. The directory structure can be escaped to read system files by adding an encoded string (payload) at subpath location.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43483	.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2024-45293	PHPSpreadsheet is a pure PHP library for reading and writing spreadsheet files. The security scanner responsible for preventing XXE attacks in the XLSX reader can be bypassed by slightly modifying the XML structure, utilizing white-spaces. On servers that allow users to upload their own Excel (XLSX) sheets, Server files and sensitive information can be disclosed by providing a crafted sheet. The security scan function in src/PhpSpreadsheet/Reader/Security/XmlScanner.php contains a flawed XML encoding check to retrieve the input file's XML encoding in the toUtf8 function. The function searches for the XML encoding through a defined regex which looks for `encoding="*"` and/or `encoding='*'`, if not found, it defaults to the UTF-8 encoding which bypasses the conversion logic. This logic can be used to pass a UTF-7 encoded XXE payload, by utilizing a whitespace before or after the = in the attribute definition. Sensitive information disclosure through the XXE on sites that allow users to upload their own excel spreadsheets, and parse them using PHPSpreadsheet's Excel parser. This issue has been addressed in release versions 1.29.1, 2.1.1, and 2.3.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2024-43484	.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2024-47654	This vulnerability exists in Shilpi Client Dashboard due to lack of rate limiting and Captcha protection for OTP requests in certain API endpoint. An unauthenticated remote attacker could exploit this vulnerability by sending multiple OTP request through vulnerable API endpoints, which could lead to the OTP bombing on the targeted system.	7.5	More Details
CVE-2024-43485	.NET and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2024-8927	In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, HTTP_REDIRECT_STATUS variable is used to check whether or not CGI binary is being run by the HTTP server. However, in certain scenarios, the content of this variable can be controlled by the request submitter via HTTP headers, which can lead to cgi.force_redirect option not being correctly applied. In certain configurations this may lead to arbitrary file inclusion in PHP.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43550	Windows Secure Channel Spoofing Vulnerability	7.4	More Details
CVE-2024-43553	NT OS Kernel Elevation of Privilege Vulnerability	7.4	More Details
CVE-2024-45246	Diebold Nixdorf – CWE-427: Uncontrolled Search Path Element	7.3	More Details
CVE-2024-21532	All versions of the package ggit are vulnerable to Command Injection via the fetchTags(branch) API, which allows user input to specify the branch to be fetched and then concatenates this string along with a git command which is then passed to the unsafe exec() Node.js child process API.	7.3	More Details
CVE-2024-9460	A vulnerability was found in Codezips Online Shopping Portal 1.0. It has been classified as critical. Affected is an unknown function of the file index.php. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-47009	Path Traversal in Ivanti Avalanche before version 6.4.5 allows a remote unauthenticated attacker to bypass authentication.	7.3	More Details
CVE-2023-6361	A vulnerability has been discovered in Winhex affecting version 16.1 SR-1 and 20.4. This vulnerability consists of a buffer overflow controlling the Structured Exception Handler (SEH) registers. This could allow attackers to execute arbitrary code via a long filename argument.	7.3	More Details
CVE-2023-6362	A vulnerability has been discovered in Winhex affecting version 16.1 SR-1 and 20.4. This vulnerability consists of a buffer overflow controlling the Structured Exception Handler (SEH) registers. This could allow attackers to execute arbitrary code via a long filename argument.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43362	Cacti is an open source performance and fault management framework. The `fileurl` parameter is not properly sanitized when saving external links in `links.php` . Morever, the said fileurl is placed in some html code which is passed to the `print` function in `link.php` and `index.php`, finally leading to stored XSS. Users with the privilege to create external links can manipulate the `fileurl` parameter in the http post request while creating external links to perform stored XSS attacks. The vulnerability known as XSS (Cross-Site Scripting) occurs when an application allows untrusted user input to be displayed on a web page without proper validation or escaping. This issue has been addressed in release version 1.2.28. All users are advised to upgrade. There are no known workarounds for this issue.	7.3	More Details
CVE-2024-47010	Path Traversal in Ivanti Avalanche before version 6.4.5 allows a remote unauthenticated attacker to bypass authentication.	7.3	More Details
CVE-2024-47610	InvenTree is an Open Source Inventory Management System. In affected versions of InvenTree it is possible for a registered user to store javascript in markdown notes fields, which are then displayed to other logged in users who visit the same page and executed. The vulnerability has been addressed as follows: 1. HTML sanitization has been enabled in the front-end markdown rendering library - `easymde`. 2. Stored markdown is also validated on the backend, to ensure that malicious markdown is not stored in the database. These changes are available in release versions 0.16.5 and later. All users are advised to upgrade. There are no workarounds, an update is required to get the new validation functions.	7.3	More Details
CVE-2024-43529	Windows Print Spooler Elevation of Privilege Vulnerability	7.3	More Details
CVE-2024-43552	Windows Shell Remote Code Execution Vulnerability	7.3	More Details
CVE-2024-47561	Schema parsing in the Java SDK of Apache Avro 1.11.3 and previous versions allows bad actors to execute arbitrary code. Users are recommended to upgrade to version 1.11.4 or 1.12.0, which fix this issue.	7.3	More Details
CVE-2024-9381	Path traversal in Ivanti CSA before version 5.0.2 allows a remote authenticated attacker with admin privileges to bypass restrictions.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20470	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system.	7.2	More Details
CVE-2024-45330	A use of externally-controlled format string in Fortinet FortiAnalyzer versions 7.4.0 through 7.4.3, 7.2.2 through 7.2.5 allows attacker to escalate its privileges via specially crafted requests.	7.2	More Details
CVE-2024-9380	An OS command injection vulnerability in the admin web console of Ivanti CSA before version 5.0.2 allows a remote authenticated attacker with admin privileges to obtain remote code execution.	7.2	More Details
CVE-2024-9314	The Rank Math SEO – AI SEO Tools to Dominate SEO Rankings plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.0.228 via deserialization of untrusted input 'set_redirections' function. This makes it possible for authenticated attackers, with Administrator-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.	7.2	More Details
CVE-2024-44030	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Mestres do WP Checkout Mestres WP allows PHP Local File Inclusion.This issue affects Checkout Mestres WP: from n/a through 8.6.	7.2	More Details
CVE-2024-43363	Cacti is an open source performance and fault management framework. An admin user can create a device with a malicious hostname containing php code and repeat the installation process (completing only step 5 of the installation process is enough, no need to complete the steps before or after it) to use a php file as the cacti log file. After having the malicious hostname end up in the logs (log poisoning), one can simply go to the log file url to execute commands to achieve RCE. This issue has been addressed in version 1.2.28 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47910	An issue was discovered in SonarSource SonarQube before 9.9.5 LTA and 10.x before 10.5. A SonarQube user with the Administrator role can modify an existing configuration of a GitHub integration to exfiltrate a pre-signed JWT.	7.2	More Details
CVE-2024-47327	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Eyal Fitoussi GEO my WordPress allows Reflected XSS.This issue affects GEO my WordPress: from n/a through 4.5.0.3.	7.1	More Details
CVE-2024-47346	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tribulant Newsletters allows Reflected XSS.This issue affects Newsletters: from n/a through 4.9.9.1.	7.1	More Details
CVE-2024-47341	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Lester ‘GaMerZ’ Chan WP-DownloadManager allows Reflected XSS.This issue affects WP-DownloadManager: from n/a through 1.68.8.	7.1	More Details
CVE-2024-47339	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in James Ward WP Mail Catcher allows Reflected XSS.This issue affects WP Mail Catcher: from n/a through 2.1.9.	7.1	More Details
CVE-2024-47360	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Booking Algorithms BA Book Everything allows Reflected XSS.This issue affects BA Book Everything: from n/a through 1.6.20.	7.1	More Details
CVE-2024-47326	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ILLID Share This Image allows Reflected XSS.This issue affects Share This Image: from n/a through 2.01.	7.1	More Details
CVE-2024-38097	Azure Monitor Agent Elevation of Privilege Vulnerability	7.1	More Details
CVE-2024-47367	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in YITH YITH WooCommerce Product Add-Ons allows Reflected XSS.This issue affects YITH WooCommerce Product Add-Ons: from n/a through 4.13.0.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47348	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WaspThemes YellowPencil Visual CSS Style Editor allows Reflected XSS.This issue affects YellowPencil Visual CSS Style Editor: from n/a through 7.6.4.	7.1	More Details
CVE-2024-43502	Windows Kernel Elevation of Privilege Vulnerability	7.1	More Details
CVE-2024-47374	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LiteSpeed Technologies LiteSpeed Cache allows Stored XSS.This issue affects LiteSpeed Cache: from n/a through 6.5.0.2.	7.1	More Details
CVE-2024-47347	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Chart Builder Team Chartify allows Reflected XSS.This issue affects Chartify: from n/a through 2.7.6.	7.1	More Details
CVE-2024-47297	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CodePeople CP Polls allows Reflected XSS.This issue affects CP Polls: from n/a through 1.0.74.	7.1	More Details
CVE-2024-47349	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPMobile.App allows Reflected XSS.This issue affects WPMobile.App: from n/a through 11.50.	7.1	More Details
CVE-2024-47352	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Xylus Themes WP Bulk Delete allows Reflected XSS.This issue affects WP Bulk Delete: from n/a through 1.3.1.	7.1	More Details
CVE-2024-20659	Windows Hyper-V Security Feature Bypass Vulnerability	7.1	More Details
CVE-2024-45454	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) allows Reflected XSS.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 1.5.121.	7.1	More Details
CVE-2024-43581	Microsoft OpenSSH for Windows Remote Code Execution Vulnerability	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47300	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CubeWP CubeWP Forms – All-in-One Form Builder allows Stored XSS.This issue affects CubeWP Forms – All-in-One Form Builder: from n/a through 1.1.1.	7.1	More Details
CVE-2024-47301	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Bit Form Bit Form – Contact Form Plugin allows Stored XSS.This issue affects Bit Form – Contact Form Plugin: from n/a through 2.13.10.	7.1	More Details
CVE-2024-47306	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Copy Content Protection Team Secure Copy Content Protection and Content Locking allows Stored XSS.This issue affects Secure Copy Content Protection and Content Locking: from n/a through 4.2.3.	7.1	More Details
CVE-2024-47320	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WS Form WS Form LITE allows Stored XSS.This issue affects WS Form LITE: from n/a through 1.9.238.	7.1	More Details
CVE-2024-47322	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ex-Themes WP Timeline – Vertical and Horizontal timeline plugin allows Reflected XSS.This issue affects WP Timeline – Vertical and Horizontal timeline plugin: from n/a through 3.6.7.	7.1	More Details
CVE-2024-44028	Cross-Site Request Forgery (CSRF) vulnerability in Nicejob NiceJob allows Stored XSS.This issue affects NiceJob: from n/a before 3.6.5.	7.1	More Details
CVE-2024-44029	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in David Garlitz viala allows Reflected XSS.This issue affects viala: from n/a through 1.3.1.	7.1	More Details
CVE-2024-9005	CWE-502: Deserialization of Untrusted Data vulnerability exists that could allow code to be remotely executed on the server when unsafely deserialized data is posted to the web server.	7.1	More Details
CVE-2024-47624	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BannerSky BSK Forms Blacklist allows Reflected XSS.This issue affects BSK Forms Blacklist: from n/a through 3.8.1.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45060	PHPSpreadsheet is a pure PHP library for reading and writing spreadsheet files. One of the sample scripts in PhpSpreadsheet is susceptible to a cross-site scripting (XSS) vulnerability due to improper handling of input where a number is expected leading to formula injection. The code in in `45_Quadratic_equation_solver.php` concatenates the user supplied parameters directly into spreadsheet formulas. This allows an attacker to take control over the formula and output unsanitized data into the page, resulting in JavaScript execution. This issue has been addressed in release versions 1.29.2, 2.1.1, and 2.3.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	7.1	More Details
CVE-2024-47369	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPWeb Social Auto Poster allows Reflected XSS.This issue affects Social Auto Poster: from n/a through 5.3.15.	7.1	More Details
CVE-2024-47333	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Team Tangible Loops & Logic allows Reflected XSS.This issue affects Loops & Logic: from n/a through 4.1.4.	7.1	More Details
CVE-2024-47644	Cross-Site Request Forgery (CSRF) vulnerability in Copyscape / Indigo Stream Technologies Copyscape Premium allows Stored XSS.This issue affects Copyscape Premium: from n/a through 1.3.6.	7.1	More Details
CVE-2024-47388	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SliceWP allows Reflected XSS.This issue affects SliceWP: from n/a through 1.1.18.	7.1	More Details
CVE-2024-47386	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 3.0.8.	7.1	More Details
CVE-2024-47384	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Compress WP Compress – Image Optimizer [All-In-One] allows Reflected XSS.This issue affects WP Compress – Image Optimizer [All-In-One]: from n/a through 6.20.13.	7.1	More Details
CVE-2024-47638	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in vCita 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 4.4.6.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47380	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Lab WP-Lister Lite for eBay allows Reflected XSS.This issue affects WP-Lister Lite for eBay: from n/a through 3.6.3.	7.1	More Details
CVE-2024-43615	Microsoft OpenSSH for Windows Remote Code Execution Vulnerability	7.1	More Details
CVE-2024-47379	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Sale php scripts Web Directory Free allows Reflected XSS.This issue affects Web Directory Free: from n/a through 1.7.3.	7.1	More Details
CVE-2024-47378	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPCOM WPCOM Member allows Reflected XSS.This issue affects WPCOM Member: from n/a through 1.5.4.	7.1	More Details
CVE-2024-47389	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Basix NEX-Forms – Ultimate Form Builder allows Reflected XSS.This issue affects NEX-Forms – Ultimate Form Builder: from n/a through 8.7.3.	7.1	More Details
CVE-2024-47394	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in eyecix JobSearch allows Reflected XSS.This issue affects JobSearch: from n/a through 2.5.9.	7.1	More Details
CVE-2024-47395	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Robokassa Robokassa payment gateway for Woocommerce allows Reflected XSS.This issue affects Robokassa payment gateway for Woocommerce: from n/a through 1.6.1.	7.1	More Details
CVE-2024-9576	Vulnerability in Distro Linux Workbooth v2.5 that allows to escalate privileges to the root user by manipulating the network configuration script.	7.0	More Details
CVE-2024-43522	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-43511	Windows Kernel Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47975	Improper access control validation in firmware of some Solidigm DC Products may allow an attacker with physical access to gain unauthorized access or an attacker with local access to potentially enable denial of service.	7.0	More Details
CVE-2024-31449	Redis is an open source, in-memory database that persists on disk. An authenticated user may use a specially crafted Lua script to trigger a stack buffer overflow in the bit library, which may potentially lead to remote code execution. The problem exists in all versions of Redis with Lua scripting. This problem has been fixed in Redis versions 6.2.16, 7.2.6, and 7.4.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.0	More Details
CVE-2024-43535	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-43612	Power BI Report Server Spoofing Vulnerability	6.9	More Details
CVE-2024-47616	Pomerium is an identity and context-aware access proxy. The Pomerium databroker service is responsible for managing all persistent Pomerium application state. Requests to the databroker service API are authorized by the presence of a JSON Web Token (JWT) signed by a key known by all Pomerium services in the same deployment. However, incomplete validation of this JWT meant that some service account access tokens would incorrectly be treated as valid for the purpose of databroker API authorization. Improper access to the databroker API could allow exfiltration of user info, spoofing of user sessions, or tampering with Pomerium routes, policies, and other settings. A Pomerium deployment is susceptible to this issue if all of the following conditions are met, you have issued a service account access token using Pomerium Zero or Pomerium Enterprise, the access token has an explicit expiration date in the future, and the core Pomerium databroker gRPC API is not otherwise secured by network access controls. This vulnerability is fixed in 0.27.1.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20524	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	6.8	More Details
CVE-2024-20523	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	6.8	More Details
CVE-2024-41585	DrayTek Vigor3910 devices through 4.3.2.6 are affected by an OS command injection vulnerability that allows an attacker to leverage the recvCmd binary to escape from the emulated instance and inject arbitrary commands into the host machine.	6.8	More Details
CVE-2024-43543	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-8743	The Bit File Manager – 100% Free & Open Source File Manager and Code Editor for WordPress plugin for WordPress is vulnerable to Limited JavaScript File Upload in all versions up to, and including, 6.5.7. This is due to a lack of proper checks on allowed file types. This makes it possible for authenticated attackers, with Subscriber-level access and above, and granted permissions by an administrator, to upload .css and .js files, which could lead to Stored Cross-Site Scripting.	6.8	More Details
CVE-2024-43523	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43526	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-43524	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-43525	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-20516	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	6.8	More Details
CVE-2024-43536	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-20517	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	6.8	More Details
CVE-2024-47911	In SonarSource SonarQube 10.4 through 10.5 before 10.6, a vulnerability was discovered in the authorizations/group-memberships API endpoint that allows SonarQube users with the administrator role to inject blind SQL commands.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47194	A vulnerability has been identified in ModelSim (All versions < V2024.3), Questa (All versions < V2024.3). vish2.exe in affected applications allows a specific DLL file to be loaded from the current working directory. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges in installations where administrators or processes with elevated privileges launch vish2.exe from a user-writable directory.	6.7	More Details
CVE-2024-20099	In power, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08997492; Issue ID: MSV-1625.	6.7	More Details
CVE-2024-47195	A vulnerability has been identified in ModelSim (All versions < V2024.3), Questa (All versions < V2024.3). gdb.exe in affected applications allows a specific executable file to be loaded from the current working directory. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges in installations where administrators or processes with elevated privileges launch gdb.exe from a user-writable directory.	6.7	More Details
CVE-2024-47196	A vulnerability has been identified in ModelSim (All versions < V2024.3), Questa (All versions < V2024.3). vsimk.exe in affected applications allows a specific tcl file to be loaded from the current working directory. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges in installations where administrators or processes with elevated privileges launch vsimk.exe from a user-writable directory.	6.7	More Details
CVE-2024-47976	Improper access removal handling in firmware of some Solidigm DC Products may allow an attacker with physical access to gain unauthorized access.	6.7	More Details
CVE-2024-3506	A possible buffer overflow in selected cameras' drivers from XProtect Device Pack can allow an attacker with access to internal network to execute commands on Recording Server under strict conditions.	6.7	More Details
CVE-2024-20090	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1703.	6.7	More Details
CVE-2024-37982	Windows Resume Extensible Firmware Interface Security Feature Bypass Vulnerability	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20098	In power, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996886; Issue ID: MSV-1626.	6.7	More Details
CVE-2024-37983	Windows Resume Extensible Firmware Interface Security Feature Bypass Vulnerability	6.7	More Details
CVE-2024-23370	Memory corruption when a process invokes IOCTL calls from user-space to create a HAB virtual channel and another process invokes IOCTL calls to destroy the same.	6.7	More Details
CVE-2024-23374	Memory corruption is possible when an attempt is made from userspace or console to write some haptics effects pattern to the haptics debugfs file.	6.7	More Details
CVE-2024-37979	Windows Kernel Elevation of Privilege Vulnerability	6.7	More Details
CVE-2024-37976	Windows Resume Extensible Firmware Interface Security Feature Bypass Vulnerability	6.7	More Details
CVE-2024-23375	Memory corruption during the network scan request.	6.7	More Details
CVE-2024-23379	Memory corruption while unmapping the fastrpc map when two threads can free the same map in concurrent scenario.	6.7	More Details
CVE-2024-23376	Memory corruption while sending the persist buffer command packet from the user-space to the kernel space through the IOCTL call.	6.7	More Details
CVE-2024-42027	The E2EE password entropy generated by Rocket.Chat Mobile prior to version 4.5.1 is insufficient, allowing attackers to crack it if they have the appropriate time and resources.	6.7	More Details
CVE-2024-23378	Memory corruption while invoking IOCTL calls for MSM module from the user space during audio playback and record.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43480	Azure Service Fabric for Linux Remote Code Execution Vulnerability	6.6	More Details
CVE-2024-47309	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Condless Cities Shipping Zones for WooCommerce allows PHP Local File Inclusion.This issue affects Cities Shipping Zones for WooCommerce: from n/a through 1.2.7.	6.6	More Details
CVE-2024-45933	OnlineNewsSite v1.0 is vulnerable to Cross Site Scripting (XSS) which allows attackers to execute arbitrary code via the Title and summary fields in the /admin/post/edit/ endpoint.	6.6	More Details
CVE-2023-26771	Taskcafe 0.3.2 is vulnerable to Cross Site Scripting (XSS). There is a lack of validation in the filetype when uploading a SVG profile picture with a XSS payload on it. An authenticated attacker can exploit this vulnerability by uploading a malicious picture which will trigger the payload when the victim opens the file.	6.5	More Details
CVE-2024-47772	Discourse is an open source platform for community discussion. An attacker can execute arbitrary JavaScript on users' browsers by sending a maliciously crafted chat message and replying to it. This issue only affects sites with CSP disabled. This problem is patched in the latest version of Discourse. All users are advised to upgrade. Users unable to upgrade should ensure CSP is enabled on the forum. Users who do upgrade should also consider enabling a CSP as well as a proactive measure.	6.5	More Details
CVE-2024-7801	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Microchip TimeProvider 4100 (Data plot modules) allows SQL Injection.This issue affects TimeProvider 4100: from 1.0 before 2.4.7.	6.5	More Details
CVE-2024-43573	Windows MSHTML Platform Spoofing Vulnerability	6.5	More Details
CVE-2024-46040	IoT Haat Smart Plug IH-IN-16A-S IH-IN-16A-S v5.16.1 suffers from Insufficient Session Expiration. The lack of validation of the authentication token at the IoT Haat during the Access Point Pairing mode leads the attacker to replay the Wi-Fi packets and forcefully turn off the access point after the authentication token has expired.	6.5	More Details
CVE-2024-47971	Improper error handling in firmware of some SSD DC Products may allow an attacker to enable denial of service.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47657	This vulnerability exists in the Shilpi Net Back Office due to improper access controls on certain API endpoints. An authenticated remote attacker could exploit this vulnerability by manipulating a parameter dfclientid through API request URLs which could lead to unauthorized access to sensitive information belonging to other users.	6.5	More Details
CVE-2024-47653	This vulnerability exists in Shilpi Client Dashboard due to lack of authorization for modification and cancellation requests through certain API endpoints. An authenticated remote attacker could exploit this vulnerability by placing or cancelling requests through API request body leading to unauthorized modification of requests belonging to the other users.	6.5	More Details
CVE-2024-47651	This vulnerability exists in Shilpi Client Dashboard due to improper handling of multiple parameters in the API endpoint. An authenticated remote attacker could exploit this vulnerability by including multiple “userid” parameters in the API request body leading to unauthorized access of sensitive information belonging to other users.	6.5	More Details
CVE-2024-45919	A security flaw has been discovered in Solvait version 24.4.2 that allows an attacker to elevate their privileges. By manipulating the Request ID and Action Type parameters in /AssignToMe/SetAction, an attacker can bypass approval workflows leading to unauthorized access to sensitive information or approval of fraudulent requests.	6.5	More Details
CVE-2024-47622	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ILLID Advanced Woo Labels allows Stored XSS.This issue affects Advanced Woo Labels: from n/a through 2.01.	6.5	More Details
CVE-2024-47818	Saltcorn is an extensible, open source, no-code database application builder. A logged-in user with any role can delete arbitrary files on the filesystem by calling the `sync/clean_sync_dir` endpoint. The `dir_name` POST parameter is not validated/sanitized and is used to construct the `syncDir` that is deleted by calling `fs.rm`. This issue has been addressed in release version 1.0.0-beta16 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2024-43561	Windows Mobile Broadband Driver Denial of Service Vulnerability	6.5	More Details
CVE-2024-43534	Windows Graphics Component Information Disclosure Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43512	Windows Standards-Based Storage Management Service Denial of Service Vulnerability	6.5	More Details
CVE-2024-35294	An unauthenticated remote attacker may use the devices traffic capture without authentication to grab plaintext administrative credentials.	6.5	More Details
CVE-2024-8037	Vulnerable juju hook tool abstract UNIX domain socket. When combined with an attack of JUJU_CONTEXT_ID, any user on the local system with access to the default network namespace may connect to the @/var/lib/juju/agents/unit-xxxx-yyyy/agent.socket and perform actions that are normally reserved to a juju charm.	6.5	More Details
CVE-2024-20365	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root.	6.5	More Details
CVE-2024-43481	Power BI Report Server Spoofing Vulnerability	6.5	More Details
CVE-2024-20515	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability is due to a lack of proper data protection mechanisms for certain configuration settings. An attacker with Read-Only Administrator privileges could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to view device credentials that are normally not visible to Read-Only Administrators.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20518	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. 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 on the underlying operating system as the root user.	6.5	More Details
CVE-2024-20519	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. 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 on the underlying operating system as the root user.	6.5	More Details
CVE-2024-20520	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. 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 on the underlying operating system as the root user.	6.5	More Details
CVE-2024-20521	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. 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 on the underlying operating system as the root user.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20522	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	6.5	More Details
CVE-2024-9379	SQL injection in the admin web console of Ivanti CSA before version 5.0.2 allows a remote authenticated attacker with admin privileges to run arbitrary SQL statements.	6.5	More Details
CVE-2024-43540	Windows Mobile Broadband Driver Denial of Service Vulnerability	6.5	More Details
CVE-2024-43542	Windows Mobile Broadband Driver Denial of Service Vulnerability	6.5	More Details
CVE-2024-46977	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. A path traversal vulnerability inside of LocalMode's open_local_file method allows an authenticated user with adequate permissions to download any .txt via the ScreensController#show on the web server COSMOS is running on (depending on the file permissions). This vulnerability is fixed in 5.19.0.	6.5	More Details
CVE-2024-47529	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. OpenC3 COSMOS stores the password of a user unencrypted in the LocalStorage of a web browser. This makes the user password susceptible to exfiltration via Cross-site scripting (see GHSL-2024-128). This vulnerability is fixed in 5.19.0. This only affects Open Source edition, and not OpenC3 COSMOS Enterprise Edition.	6.5	More Details
CVE-2024-9100	Zohocorp ManageEngine Analytics Plus versions before 5410 and Zoho Analytics On-Premise versions before 5410 are vulnerable to Path traversal.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45870	Bandisoft BandiView 7.05 is vulnerable to Incorrect Access Control in sub_0x3d80fc via a crafted POC file.	6.5	More Details
CVE-2024-43609	Microsoft Office Spoofing Vulnerability	6.5	More Details
CVE-2024-43555	Windows Mobile Broadband Driver Denial of Service Vulnerability	6.5	More Details
CVE-2024-21533	All versions of the package ggit are vulnerable to Arbitrary Argument Injection via the clone() API, which allows specifying the remote URL to clone and the file on disk to clone to. The library does not sanitize for user input or validate a given URL scheme, nor does it properly pass command-line flags to the git binary using the double-dash POSIX characters (--) to communicate the end of options.	6.5	More Details
CVE-2024-43557	Windows Mobile Broadband Driver Denial of Service Vulnerability	6.5	More Details
CVE-2024-43558	Windows Mobile Broadband Driver Denial of Service Vulnerability	6.5	More Details
CVE-2024-43559	Windows Mobile Broadband Driver Denial of Service Vulnerability	6.5	More Details
CVE-2024-43547	Windows Kerberos Information Disclosure Vulnerability	6.5	More Details
CVE-2024-43537	Windows Mobile Broadband Driver Denial of Service Vulnerability	6.5	More Details
CVE-2024-47355	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CozyThemes Cozy Blocks allows Stored XSS.This issue affects Cozy Blocks: from n/a through 2.0.11.	6.5	More Details
CVE-2024-47625	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeLooks Enter Addons allows Stored XSS.This issue affects Enter Addons: from n/a through 2.1.8.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43538	Windows Mobile Broadband Driver Denial of Service Vulnerability	6.5	More Details
CVE-2024-47340	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PickPlugins Post Grid and Gutenberg Blocks allows Stored XSS.This issue affects Post Grid and Gutenberg Blocks: from n/a through 2.2.89.	6.5	More Details
CVE-2024-47342	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PickPlugins Accordion accordions allows Stored XSS.This issue affects Accordion: from n/a through 2.2.99.	6.5	More Details
CVE-2024-47343	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kraftplugins Mega Elements allows Stored XSS.This issue affects Mega Elements: from n/a through 1.2.4.	6.5	More Details
CVE-2024-47382	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Webvitaly Page-list allows Stored XSS.This issue affects Page-list: from n/a through 5.6.	6.5	More Details
CVE-2024-47630	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 1.2.7.	6.5	More Details
CVE-2024-47629	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BdThemes Ultimate Store Kit Elementor Addons allows Stored XSS.This issue affects Ultimate Store Kit Elementor Addons: from n/a through 2.0.5.	6.5	More Details
CVE-2024-47628	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LA-Studio LA-Studio Element Kit for Elementor allows Stored XSS.This issue affects LA-Studio Element Kit for Elementor: from n/a through 1.3.9.3.	6.5	More Details
CVE-2024-47627	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Travel WP Travel Gutenberg Blocks allows Stored XSS.This issue affects WP Travel Gutenberg Blocks: from n/a through 3.6.0.	6.5	More Details
CVE-2024-47298	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BoldThemes Bold Page Builder allows Stored XSS.This issue affects Bold Page Builder: from n/a through 5.1.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47626	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Rometheme RomethemeKit For Elementor allows Stored XSS.This issue affects RomethemeKit For Elementor: from n/a through 1.5.0.	6.5	More Details
CVE-2024-47307	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Essential Plugin Meta slider and carousel with lightbox allows Stored XSS.This issue affects Meta slider and carousel with lightbox: from n/a through 2.0.1.	6.5	More Details
CVE-2024-47329	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in QuomodoSoft ElementsReady Addons for Elementor allows Stored XSS.This issue affects ElementsReady Addons for Elementor: from n/a through 6.4.0.	6.5	More Details
CVE-2024-44035	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 1.3.7.	6.5	More Details
CVE-2024-47310	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ARI Soft ARI Fancy Lightbox allows Stored XSS.This issue affects ARI Fancy Lightbox: from n/a through 1.3.17.	6.5	More Details
CVE-2024-47643	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Alexander Böhm Include Fussball.De Widgets allows Stored XSS.This issue affects Include Fussball.De Widgets: from n/a through 4.0.0.	6.5	More Details
CVE-2024-44022	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Trustmary Review & testimonial widgets allows Stored XSS.This issue affects Review & testimonial widgets: from n/a through 1.0.5.	6.5	More Details
CVE-2024-44024	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NicheAddons Medical Addon for Elementor allows Stored XSS.This issue affects Medical Addon for Elementor: from n/a through 1.4.	6.5	More Details
CVE-2024-44025	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Nicejob NiceJob allows Stored XSS.This issue affects NiceJob: from n/a before 3.6.5.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44026	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NicheAddons Charity Addon for Elementor allows Stored XSS.This issue affects Charity Addon for Elementor: from n/a through 1.3.0.	6.5	More Details
CVE-2024-44027	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 1.3.6.	6.5	More Details
CVE-2024-44033	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NicheAddons Primary Addon for Elementor allows Stored XSS.This issue affects Primary Addon for Elementor: from n/a through 1.5.7.	6.5	More Details
CVE-2024-44032	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NicheAddons Restaurant & Cafe Addon for Elementor allows Stored XSS.This issue affects Restaurant & Cafe Addon for Elementor: from n/a through 1.5.5.	6.5	More Details
CVE-2024-47642	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Keap Keap Official Opt-in Forms allows Stored XSS.This issue affects Keap Official Opt-in Forms: from n/a through 2.0.1.	6.5	More Details
CVE-2024-47332	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in wowDevs Sky Addons for Elementor allows Stored XSS.This issue affects Sky Addons for Elementor: from n/a through 2.5.11.	6.5	More Details
CVE-2024-47639	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in VdoCipher allows Stored XSS.This issue affects VdoCipher: from n/a through 1.29.	6.5	More Details
CVE-2024-47385	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloper Essential Blocks for Gutenberg allows Stored XSS.This issue affects Essential Blocks for Gutenberg: from n/a through 4.8.4.	6.5	More Details
CVE-2024-47650	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Axton WP-WebAuthn allows Stored XSS.This issue affects WP-WebAuthn: from n/a through 1.3.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47392	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BdThemes Element Pack Elementor Addons allows Stored XSS.This issue affects Element Pack Elementor Addons: from n/a through 5.7.5.	6.5	More Details
CVE-2024-47391	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BoldThemes Bold Page Builder allows Stored XSS.This issue affects Bold Page Builder: from n/a before 5.1.1.	6.5	More Details
CVE-2024-47368	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 2.1.33.	6.5	More Details
CVE-2024-47357	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Leevio Happy Addons for Elementor allows Stored XSS.This issue affects Happy Addons for Elementor: from n/a through 3.12.0.	6.5	More Details
CVE-2024-47375	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ashraf XLTab – Accordions and Tabs for Elementor Page Builder allows Stored XSS.This issue affects XLTab – Accordions and Tabs for Elementor Page Builder: from n/a through 1.3.	6.5	More Details
CVE-2024-47373	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LiteSpeed Technologies LiteSpeed Cache allows Stored XSS.This issue affects LiteSpeed Cache: from n/a through 6.5.0.2.	6.5	More Details
CVE-2024-47390	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jegtheme Jeg Elementor Kit allows Stored XSS.This issue affects Jeg Elementor Kit: from n/a through 2.6.8.	6.5	More Details
CVE-2024-47631	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in bPlugins LLC Logo Carousel – Clients logo carousel for WP allows Stored XSS.This issue affects Logo Carousel – Clients logo carousel for WP: from n/a through 1.2.	6.5	More Details
CVE-2024-47632	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in deTheme DethemeKit For Elementor allows Stored XSS.This issue affects DethemeKit For Elementor: from n/a through 2.1.7.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9161	The Rank Math SEO – AI SEO Tools to Dominate SEO Rankings plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check on the 'update_metadata' function in all versions up to, and including, 1.0.228. This makes it possible for unauthenticated attackers to insert new and update existing metadata beginning with 'rank_math', and delete arbitrary existing user metadata and term metadata. Deleting existing usermeta can cause a loss of access to the administrator dashboard for any registered users, including Administrators.	6.5	More Details
CVE-2024-47370	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Paul Bearne Author Avatars List/Block allows Stored XSS.This issue affects Author Avatars List/Block: from n/a through 2.1.21.	6.5	More Details
CVE-2024-47633	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Zoho Forms allows Stored XSS.This issue affects Zoho Forms: from n/a through 4.0.	6.5	More Details
CVE-2024-47621	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Katie Seaborn Zotpress allows Stored XSS.This issue affects Zotpress: from n/a through 7.3.10.	6.5	More Details
CVE-2024-47363	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Blockspare allows Stored XSS.This issue affects Blockspare: from n/a through 3.2.4.	6.5	More Details
CVE-2024-47364	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Move addons Move Addons for Elementor allows Stored XSS.This issue affects Move Addons for Elementor: from n/a through 1.3.4.	6.5	More Details
CVE-2024-47365	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Atakan Au Automatically Hierarchic Categories in Menu allows Stored XSS.This issue affects Automatically Hierarchic Categories in Menu: from n/a through 2.0.5.	6.5	More Details
CVE-2024-47366	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPVibes Elementor Addon Elements allows Stored XSS.This issue affects Elementor Addon Elements: from n/a through 1.13.6.	6.5	More Details
CVE-2024-47393	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Quillforms Quill Forms allows Stored XSS.This issue affects Quill Forms: from n/a through 3.7.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9172	The Demo Importer Plus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.0.1 due to insufficient input sanitization and output escaping. 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 the SVG file.	6.4	More Details
CVE-2024-8967	The PWA — easy way to Progressive Web App plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.6.3 due to insufficient input sanitization and output escaping. 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 the SVG file.	6.4	More Details
CVE-2024-8804	The Code Embed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's script embed functionality in all versions up to, and including, 2.4 due to insufficient restrictions on who can utilize the functionality. 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-2024-8282	The Ibtana – WordPress Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘align’ attribute within the 'wp:ive/ive-productscarousel' Gutenberg block in all versions up to, and including, 1.2.4.4 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-2024-9271	The Re:WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping. 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 the SVG file.	6.4	More Details
CVE-2024-43513	BitLocker Security Feature Bypass Vulnerability	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9242	The Memberful – Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'memberful_buy_subscription_link' and 'memberful_podcasts_link' shortcodes in all versions up to, and including, 1.73.7 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-2024-43570	Windows Kernel Elevation of Privilege Vulnerability	6.4	More Details
CVE-2024-9368	The Aggregator Advanced Settings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads 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 Author-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-2024-9445	The Display Medium Posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's display_medium_posts shortcode in all versions up to, and including, 5.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9421	The Login Logout Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' parameter in all versions up to, and including, 1.1.0 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-2024-8505	The WordPress Infinite Scroll – Ajax Load More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘button_label’ parameter in all versions up to, and including, 7.1.2 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 Number	Description	Base Score	Reference
CVE-2024-9372	The WP Blocks Hub plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.2 due to insufficient input sanitization and output escaping. 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 the SVG file.	6.4	More Details
CVE-2024-9292	The Bridge Core plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'formforall' shortcode in versions up to, and including, 3.2.0 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-2024-8519	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'um_loggedin' shortcode in all versions up to, and including, 2.8.6 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-2024-8964	The Image Optimizer, Resizer and CDN – Sirv plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 7.2.9 due to insufficient input sanitization and output escaping. 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 the SVG file.	6.4	More Details
CVE-2024-8159	Deep Freeze 9.00.020.5760 is vulnerable to an out-of-bounds read vulnerability by triggering the 0x70014 IOCTL code of the FarDisk.sys driver.	6.4	More Details
CVE-2024-8433	The Easy Mega Menu Plugin for WordPress – ThemeHunk plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘themehunk_megamenu_bg_image' parameter in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Please note that this was partially fixed in 1.1.0 due to the missing authorization protection that was added.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8482	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in all versions up to, and including, 1.3.982 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-2024-47079	Meshtastic is an open source, off-grid, decentralized, mesh network built to run on affordable, low-power devices. Meshtastic firmware is an open source firmware implementation for the broader project. The remote hardware module of the firmware does not have proper checks to ensure a remote hardware control message was received should be considered valid. This issue has been addressed in release version 2.5.1. All users are advised to upgrade. There are no known workarounds for this vulnerability.	6.4	More Details
CVE-2024-9455	The WP Cleanup and Basic Functions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping. 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 the SVG file.	6.4	More Details
CVE-2024-9071	The Easy Demo Importer – A Modern One-Click Demo Import Solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.1.2 due to insufficient input sanitization and output escaping. 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 the SVG file.	6.4	More Details
CVE-2024-8486	The Shortcodes and extra features for Phlox theme plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in the Modern Heading and Icon Picker widgets all versions up to, and including, 2.16.3 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 Number	Description	Base Score	Reference
CVE-2024-20448	A vulnerability in the Cisco Nexus Dashboard Fabric Controller (NDFC) software, formerly Cisco Data Center Network Manager (DCNM), could allow an attacker with access to a backup file to view sensitive information. This vulnerability is due to the improper storage of sensitive information within config only and full backup files. An attacker could exploit this vulnerability by parsing the contents of a backup file that is generated from an affected device. A successful exploit could allow the attacker to access sensitive information, including NDFC-connected device credentials, the NDFC site manager private key, and the scheduled backup file encryption key.	6.3	More Details
CVE-2024-45291	PHPSpreadsheet is a pure PHP library for reading and writing spreadsheet files. It's possible for an attacker to construct an XLSX file that links images from arbitrary paths. When embedding images has been enabled in HTML writer with `$writer->setEmbedImages(true);` those files will be included in the output as `data:` URLs, regardless of the file's type. Also URLs can be used for embedding, resulting in a Server-Side Request Forgery vulnerability. When embedding images has been enabled, an attacker can read arbitrary files on the server and perform arbitrary HTTP GET requests. Note that any PHP protocol wrappers can be used, meaning that if for example the `expect://` wrapper is enabled, also remote code execution is possible. This issue has been addressed in release versions 1.29.2, 2.1.1, and 2.3.0. All users are advised to upgrade. there are no known workarounds for this vulnerability.	6.3	More Details
CVE-2024-9560	A vulnerability was found in ESAFENET CDG V5. It has been rated as critical. Affected by this issue is the function delCatelogs of the file /CDGServer3/document/Catelogs;logindojojs?command=DelCatelogs. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9429	A vulnerability has been found in code-projects Restaurant Reservation System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /filter2.php. The manipulation of the argument from/to leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "from" to be affected. But it must be assumed that parameter "to" is affected as well.	6.3	More Details
CVE-2024-6442	In ascs_cp_rsp_add in /subsys/bluetooth/audio/ascs.c, an unchecked tailroom could lead to a global buffer overflow.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20438	A vulnerability in the REST API endpoints of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to read or write files on an affected device. This vulnerability exists because of missing authorization controls on some REST API endpoints. An attacker could exploit this vulnerability by sending crafted API requests to an affected endpoint. A successful exploit could allow the attacker to perform limited network-admin functions such as reading device configuration information, uploading files, and modifying uploaded files. Note: This vulnerability only affects a subset of REST API endpoints and does not affect the web-based management interface.	6.3	More Details
CVE-2024-6443	In utf8_trunc in zephyr/lib/utils/utf8.c, last_byte_p can point to one byte before the string pointer if the string is empty.	6.3	More Details
CVE-2024-9573	SQL injection vulnerability in SOPlanning <1.45, through /soplanning/www/groupe_list.php, in the by parameter, which could allow a remote user to send a specially crafted query and extract all the information stored on the server.	6.3	More Details
CVE-2024-9572	Cross-Site Scripting (XSS) vulnerability in SOPlanning <1.45, due to lack of proper validation of user input via /soplanning/www/process/groupe_save.php, in the groupe_id parameter. This could allow a remote user to send a specially crafted query to an authenticated user and steal their session details.	6.3	More Details
CVE-2024-20490	A vulnerability in a logging function of Cisco Nexus Dashboard Fabric Controller (NDFC) and Cisco Nexus Dashboard Orchestrator (NDO) could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because HTTP proxy credentials could be recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view HTTP proxy server admin credentials in clear text that are configured on Nexus Dashboard to reach an external network. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information.	6.3	More Details
CVE-2024-9571	Cross-Site Scripting (XSS) vulnerability in SOPlanning <1.45, due to lack of proper validation of user input via /soplanning/www/process/xajax_server.php, affecting multiple parameters. This could allow a remote user to send a specially crafted query to an authenticated user and partially take control of their browser session.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20491	A vulnerability in a logging function of Cisco Nexus Dashboard Insights could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because remote controller credentials are recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view remote controller admin credentials in clear text. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information.	6.3	More Details
CVE-2024-9536	A vulnerability was found in ESAFENET CDG V5. It has been rated as critical. Affected by this issue is some unknown functionality of the file /MultiServerBackService?path=1. The manipulation of the argument fileId leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-6444	No proper validation of the length of user input in olcp_ind_handler in zephyr/subsys/bluetooth/services/ots/ots_client.c.	6.3	More Details
CVE-2024-45872	Bandisoft BandiView 7.05 is vulnerable to Buffer Overflow via sub_0x410d1d. The vulnerability occurs due to insufficient validation of PSD files.	6.3	More Details
CVE-2024-45871	Bandisoft BandiView 7.05 is Incorrect Access Control via sub_0x232bd8 resulting in denial of service (DOS).	6.3	More Details
CVE-2024-35215	NULL pointer dereference in IP socket options processing of the Networking Stack in QNX Software Development Platform (SDP) version(s) 7.1 and 7.0 could allow an attacker with local access to cause a denial-of-service condition in the context of the Networking Stack process.	6.2	More Details
CVE-2024-34662	Improper access control in ActivityManager prior to SMR Oct-2024 Release 1 in select Android 12, 13 and SMR Sep-2024 Release 1 in select Android 14 allows local attackers to execute privileged behaviors.	6.2	More Details
CVE-2024-47969	Improper resource management in firmware of some Solidigm DC Products may allow an attacker to potentially enable denial of service.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9237	The Fish and Ships – Most flexible shipping table rate. A WooCommerce shipping rate plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.5.9. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9207	The BuddyPress Docs plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.2.3. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-28710	Cross Site Scripting vulnerability in LimeSurvey before 6.5.0+240319 allows a remote attacker to execute arbitrary code via a lack of input validation and output encoding in the Alert Widget's message component.	6.1	More Details
CVE-2024-38038	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim’s browser.	6.1	More Details
CVE-2024-28709	Cross Site Scripting vulnerability in LimeSurvey before 6.5.12+240611 allows a remote attacker to execute arbitrary code via a crafted script to the title and comment fields.	6.1	More Details
CVE-2024-43686	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Microchip TimeProvider 4100 (data plot modules) allows Reflected XSS.This issue affects TimeProvider 4100: from 1.0 before 2.4.7.	6.1	More Details
CVE-2024-9353	The Popularis Extra plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.2.6. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9349	The Auto Amazon Links – Amazon Associates Affiliate Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 5.4.2. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-38037	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 11.0 and 10.9.1 that may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks.	6.1	More Details
CVE-2024-9204	The Smart Custom 404 Error Page plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via $_SERVER['REQUEST_URI'] in all versions up to, and including, 11.4.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-8148	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 10.8.1 - 11.2 that may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks.	6.1	More Details
CVE-2024-8802	The Clio Grow plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.0.2. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-47617	Sulu is a PHP content management system. This vulnerability allows an attacker to inject arbitrary HTML/JavaScript code through the media download URL in Sulu CMS. It affects the SuluMediaBundle component. The vulnerability is a Reflected Cross-Site Scripting (XSS) issue, which could potentially allow attackers to steal sensitive information, manipulate the website's content, or perform actions on behalf of the victim. This vulnerability is fixed in 2.6.5 and 2.5.21.	6.1	More Details
CVE-2024-38425	Information disclosure while sending implicit broadcast containing APP launch information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43683	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Microchip TimeProvider 4100 allows XSS Through HTTP Headers.This issue affects TimeProvider 4100: from 1.0.	6.1	More Details
CVE-2024-45247	Sonarr – CWE-601: URL Redirection to Untrusted Site ('Open Redirect')	6.1	More Details
CVE-2024-43687	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Microchip TimeProvider 4100 (banner config modules) allows Cross-Site Scripting (XSS).This issue affects TimeProvider 4100: from 1.0 before 2.4.7.	6.1	More Details
CVE-2024-41591	DrayTek Vigor3910 devices through 4.3.2.6 allow unauthenticated DOM-based reflected XSS.	6.1	More Details
CVE-2024-8629	The WooCommerce Multilingual & Multicurrency with WPML plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 5.3.7. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9345	The Product Delivery Date for WooCommerce – Lite plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.7.3. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. This is only exploitable when notices are present.	6.1	More Details
CVE-2024-43795	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. The login functionality contains a reflected cross-site scripting (XSS) vulnerability. This vulnerability is fixed in 5.19.0. Note: This CVE only affects Open Source Edition, and not OpenC3 COSMOS Enterprise Edition.	6.1	More Details
CVE-2024-9222	The Paid Membership Subscriptions – Effortless Memberships, Recurring Payments & Content Restriction plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.12.8. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8800	The RabbitLoader – Website Speed Optimization for improving Core Web Vital metrics with Cache, Image Optimization, and more plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.21.0. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9435	The ShiftController Employee Shift Scheduling plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via URL keys in all versions up to, and including, 4.9.66 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9375	The WordPress Captcha Plugin by Captcha Bank plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 4.0.36. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-47765	Minecraft MOTD Parser is a PHP library to parse minecraft server motd. The HtmlGenerator class is subject to potential cross-site scripting (XSS) attack through a parsed malformed Minecraft server MOTD. The HtmlGenerator iterates through objects of MotdItem that are contained in an object of MotdItemCollection to generate a HTML string. An attacker can make malicious inputs to the color and text properties of MotdItem to inject own HTML into a web page during web page generation. For example by sending a malicious MOTD from a Minecraft server under their control that was queried and passed to the HtmlGenerator. This XSS vulnerability exists because the values of these properties are neither filtered nor escaped. This vulnerability is fixed in 1.0.6.	6.1	More Details
CVE-2024-9385	The Themify Builder plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 7.6.2. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9210	The MC4WP: Mailchimp Top Bar plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.6.0. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-47781	CreateWiki is an extension used at Miraheze for requesting & creating wikis. The name of requested wikis is not escaped on Special:RequestWikiQueue, so a user can insert arbitrary HTML that is displayed in the request wiki queue when requesting a wiki. If a wiki creator comes across the XSS payload, their user session can be abused to retrieve deleted wiki requests, which typically contains private information. Likewise, this can also be abused on those with the ability to suppress requests to view sensitive information. This issue has been patched with commit `693a220` and all users are advised to apply the patch. Users unable to upgrade should disable Javascript and/or prevent access to the vulnerable page (Special:RequestWikiQueue).	6.1	More Details
CVE-2024-42831	A reflected cross-site scripting (XSS) vulnerability in Elaine's Realtime CRM Automation v6.18.17 allows attackers to execute arbitrary JavaScript code in the web browser of a user via injecting a crafted payload into the dialog parameter at wrapper_dialog.php.	6.1	More Details
CVE-2024-47817	Lara-zeus Dynamic Dashboard simple way to manage widgets for your website landing page, and filament dashboard and Lara-zeus artemis is a collection of themes for the lara-zeus ecosystem. If values passed to a paragraph widget are not valid and contain a specific set of characters, applications are vulnerable to XSS attack against a user who opens a page on which a paragraph widget is rendered. Users are advised to upgrade to the appropriate fix versions detailed in the advisory metadata. There are no known workarounds for this vulnerability.	6.1	More Details
CVE-2024-46300	itsourcecode Placement Management System 1.0 is vulnerable to Cross Site Scripting (XSS) via the Full Name field in registration.php.	6.1	More Details
CVE-2024-47847	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - Cargo allows Cross-Site Scripting (XSS).This issue affects Mediawiki - Cargo: from 3.6.X before 3.6.1.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9225	The SEOPress – On-site SEO plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 8.1.1. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-25691	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 11.1, 10.9.1 and 10.8.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim’s browser.	6.1	More Details
CVE-2024-9384	The Quantity Dynamic Pricing & Bulk Discounts for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.8.0. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9344	The BerqWP – Automated All-In-One PageSpeed Optimization Plugin for Core Web Vitals, Cache, CDN, Images, CSS, and JavaScript plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'url' parameter in all versions up to, and including, 2.1.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9417	The Hash Form – Drag & Drop Form Builder plugin for WordPress is vulnerable to limited file uploads due to a misconfigured file type validation in the 'handleUpload' function in all versions up to, and including, 1.1.9. This makes it possible for unauthenticated attackers to upload files that are excluded from both the 'allowedExtensions' and 'unallowed_extensions' arrays on the affected site's server, including files that may contain cross-site scripting.	6.1	More Details
CVE-2024-9378	The YML for Yandex Market plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'page' parameter in all versions up to, and including, 4.7.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9218	The Magazine Blocks – Blog Designer, Magazine & Newspaper Website Builder, Page Builder with Posts Blocks, Post Grid plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.3.14. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-47854	An XSS vulnerability was discovered in Veritas Data Insight before 7.1. It allows a remote attacker to inject an arbitrary web script into an HTTP request that could reflect back to an authenticated user without sanitization if executed by that user.	6.1	More Details
CVE-2024-20492	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices.	6.0	More Details
CVE-2024-44046	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themify Themify – WooCommerce Product Filter allows Stored XSS.This issue affects Themify – WooCommerce Product Filter: from n/a through 1.5.1.	5.9	More Details
CVE-2024-44039	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Travel allows Stored XSS.This issue affects WP Travel: from n/a through 9.3.1.	5.9	More Details
CVE-2024-44045	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kevon Adonis WP Abstracts allows Stored XSS.This issue affects WP Abstracts: from n/a through 2.6.5.	5.9	More Details
CVE-2024-47299	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SeedProd Coming Soon Page, Under Construction & Maintenance Mode by SeedProd allows Stored XSS.This issue affects Coming Soon Page, Under Construction & Maintenance Mode by SeedProd: from n/a through 6.17.4.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47345	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brainstorm Force Starter Templates allows Stored XSS.This issue affects Starter Templates: from n/a through 4.4.0.	5.9	More Details
CVE-2024-44042	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Fahad Mahmood WP Datepicker allows Stored XSS.This issue affects WP Datepicker: from n/a through 2.1.1.	5.9	More Details
CVE-2024-44037	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MagePeople Team Multipurpose Ticket Booking Manager allows Stored XSS.This issue affects Multipurpose Ticket Booking Manager: from n/a through 4.2.2.	5.9	More Details
CVE-2024-47383	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Webangon The Pack Elementor addons allows Stored XSS.This issue affects The Pack Elementor addons: from n/a through 2.0.8.8.	5.9	More Details
CVE-2024-47336	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Vladimir Statsenko Terms descriptions allows Stored XSS.This issue affects Terms descriptions: from n/a through 3.4.6.	5.9	More Details
CVE-2024-47371	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Walter Pinem WP MyLinks allows Stored XSS.This issue affects WP MyLinks: from n/a through 1.0.6.	5.9	More Details
CVE-2024-44041	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 8.66.	5.9	More Details
CVE-2024-44439	An issue in Shanghai Zhouma Network Technology CO., Ltd IMS Intelligent Manufacturing Collaborative Internet of Things System v.1.9.1 allows a remote attacker to escalate privileges via the open port.	5.9	More Details
CVE-2024-47387	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LinkGraph Search Atlas SEO allows Stored XSS.This issue affects Search Atlas SEO: from n/a through 1.8.2.	5.9	More Details
CVE-2024-34535	In Mastodon 4.1.6, API endpoint rate limiting can be bypassed by setting a crafted HTTP request header.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47372	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeNcode LLC TNC PDF viewer allows Stored XSS.This issue affects TNC PDF viewer: from n/a through 3.1.0.	5.9	More Details
CVE-2024-47623	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in GhozyLab, Inc. Gallery Lightbox allows Stored XSS.This issue affects Gallery Lightbox: from n/a through 1.0.0.39.	5.9	More Details
CVE-2024-47647	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in HelpieWP Accordion & FAQ – Helpie WordPress Accordion FAQ Plugin allows Stored XSS.This issue affects Accordion & FAQ – Helpie WordPress Accordion FAQ Plugin: from n/a through 1.27.	5.9	More Details
CVE-2024-47381	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Averta Depicter Slider allows Stored XSS.This issue affects Depicter Slider: from n/a through 3.2.2.	5.9	More Details
CVE-2024-44040	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Plainware ShiftController Employee Shift Scheduling allows Stored XSS.This issue affects ShiftController Employee Shift Scheduling: from n/a through 4.9.64.	5.9	More Details
CVE-2024-47376	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tribulant Slideshow Gallery allows Stored XSS.This issue affects Slideshow Gallery: from n/a through 1.8.3.	5.9	More Details
CVE-2024-44043	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in 10Web Photo Gallery by 10Web allows Stored XSS.This issue affects Photo Gallery by 10Web: from n/a through 1.8.27.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20385	A vulnerability in the SSL/TLS implementation of Cisco Nexus Dashboard Orchestrator (NDO) could allow an unauthenticated, remote attacker to intercept sensitive information from an affected device. This vulnerability exists because the Cisco NDO Validate Peer Certificate site management feature validates the certificates for Cisco Application Policy Infrastructure Controller (APIC), Cisco Cloud Network Controller (CNC), and Cisco Nexus Dashboard only when a new site is added or an existing one is reregistered. An attacker could exploit this vulnerability by using machine-in-the-middle techniques to intercept the traffic between the affected device and Cisco NDO and then using a crafted certificate to impersonate the affected device. A successful exploit could allow the attacker to learn sensitive information during communications between these devices.	5.9	More Details
CVE-2024-44036	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pierre Lebedel Kodex Posts likes allows Stored XSS.This issue affects Kodex Posts likes: from n/a through 2.5.0.	5.9	More Details
CVE-2024-47377	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeKraft BuddyForms allows Stored XSS.This issue affects BuddyForms: from n/a through 2.8.12.	5.9	More Details
CVE-2024-47762	Backstage is an open framework for building developer portals. Configuration supplied through APP_CONFIG_* environment variables, for example APP_CONFIG_backend_listen_port=7007, where unexpectedly ignoring the visibility defined in configuration schema. This occurred even if the configuration schema specified that they should have backend or secret visibility. This was an intended feature of the APP_CONFIG_* way of supplying configuration, but now clearly goes against the expected behavior of the configuration system. This behavior leads to a risk of potentially exposing sensitive configuration details intended to remain private or restricted to backend processes. The issue has been resolved in version 0.3.75 of the @backstage/plugin-app-backend package. As a temporary measure, avoid supplying secrets using the APP_CONFIG_ configuration pattern. Consider alternative methods for setting secrets, such as the environment substitution available for Backstage configuration.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20513	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate.	5.8	More Details
CVE-2024-20500	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.	5.8	More Details
CVE-2024-20502	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20509	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device.	5.8	More Details
CVE-2024-43604	Outlook for Android Elevation of Privilege Vulnerability	5.7	More Details
CVE-2024-43364	Cacti is an open source performance and fault management framework. The `title` parameter is not properly sanitized when saving external links in links.php . Morever, the said title parameter is stored in the database and reflected back to user in index.php, finally leading to stored XSS. Users with the privilege to create external links can manipulate the `title` parameter in the http post request while creating external links to perform stored XSS attacks. The vulnerability known as XSS (Cross-Site Scripting) occurs when an application allows untrusted user input to be displayed on a web page without proper validation or escaping. This issue has been addressed in release version 1.2.28. All users are advised to upgrade. There are no known workarounds for this vulnerability.	5.7	More Details
CVE-2024-43365	Cacti is an open source performance and fault management framework. The`consolenewsection` parameter is not properly sanitized when saving external links in links.php . Morever, the said consolenewsection parameter is stored in the database and reflected back to user in `index.php`, finally leading to stored XSS. Users with the privilege to create external links can manipulate the “consolenewsection” parameter in the http post request while creating external links to perform stored XSS attacks. The vulnerability known as XSS (Cross-Site Scripting) occurs when an application allows untrusted user input to be displayed on a web page without proper validation or escaping. This issue has been addressed in release version 1.2.28. All users are advised to upgrade. There are no known workarounds for this vulnerability.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20441	A vulnerability in a specific REST API endpoint of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to learn sensitive information on an affected device. This vulnerability is due to insufficient authorization controls on the affected REST API endpoint. An attacker could exploit this vulnerability by sending crafted API requests to the affected endpoint. A successful exploit could allow the attacker to download config only or full backup files and learn sensitive configuration information. This vulnerability only affects a specific REST API endpoint and does not affect the web-based management interface.	5.7	More Details
CVE-2024-44674	D-Link COVR-2600R FW101b05 is vulnerable to Buffer Overflow. In the function sub_24E28, the HTTP_REFERER is obtained through an environment variable, and this field is controllable, allowing it to be used as the value for src.	5.7	More Details
CVE-2024-43571	Sudo for Windows Spoofing Vulnerability	5.6	More Details
CVE-2024-43546	Windows Cryptographic Information Disclosure Vulnerability	5.6	More Details
CVE-2024-43585	Code Integrity Guard Security Feature Bypass Vulnerability	5.5	More Details
CVE-2024-43614	Microsoft Defender for Endpoint for Linux Spoofing Vulnerability	5.5	More Details
CVE-2024-20444	A vulnerability in Cisco Nexus Dashboard Fabric Controller (NDFC), formerly Cisco Data Center Network Manager (DCNM), could allow an authenticated, remote attacker with network-admin privileges to perform a command injection attack against an affected device. This vulnerability is due to insufficient validation of command arguments. An attacker could exploit this vulnerability by submitting crafted command arguments to a specific REST API endpoint. A successful exploit could allow the attacker to overwrite sensitive files or crash a specific container, which would restart on its own, causing a low-impact denial of service (DoS) condition.	5.5	More Details
CVE-2024-43500	Windows Resilient File System (ReFS) Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43508	Windows Graphics Component Information Disclosure Vulnerability	5.5	More Details
CVE-2024-34672	Improper input validation in SamsungVideoPlayer prior to versions 7.3.29.1 in Android 12, 7.3.36.1 in Android 13, and 7.3.41.230 in Android 14 allows local attackers to access video file of other users.	5.5	More Details
CVE-2024-43554	Windows Kernel-Mode Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2024-31228	Redis is an open source, in-memory database that persists on disk. Authenticated users can trigger a denial-of-service by using specially crafted, long string match patterns on supported commands such as `KEYS`, `SCAN`, `PSUBSCRIBE`, `FUNCTION LIST`, `COMMAND LIST` and ACL definitions. Matching of extremely long patterns may result in unbounded recursion, leading to stack overflow and process crash. This problem has been fixed in Redis versions 6.2.16, 7.2.6, and 7.4.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.5	More Details
CVE-2024-39806	in OpenHarmony v4.1.0 and prior versions allow a local attacker cause information leak through out-of-bounds Read.	5.5	More Details
CVE-2024-44204	A logic issue was addressed with improved validation. This issue is fixed in iOS 18.0.1 and iPadOS 18.0.1. A user's saved passwords may be read aloud by VoiceOver.	5.5	More Details
CVE-2024-43603	Visual Studio Collector Service Denial of Service Vulnerability	5.5	More Details
CVE-2024-46325	TP-Link WR740N V6 has a stack overflow vulnerability via the ssid parameter in /userRpm/popupSiteSurveyRpm.htm url.	5.5	More Details
CVE-2024-47635	Cross-Site Request Forgery (CSRF) vulnerability in TinyPNG.This issue affects TinyPNG: from n/a through 3.4.3.	5.4	More Details
CVE-2024-46077	itsourcecode Online Tours and Travels Management System v1.0 is vulnerable to Cross Site Scripting (XSS) via a crafted payload to the val-username, val-email, val-suggestions, val-digits and state_name parameters in travellers.php.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33209	FlatPress v1.3 is vulnerable to Cross Site Scripting (XSS). An attacker can inject malicious JavaScript code into the "Add New Entry" section, which allows them to execute arbitrary code in the context of a victim's web browser.	5.4	More Details
CVE-2024-47594	SAP NetWeaver Enterprise Portal (KMC) does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting vulnerability in KMC servlet. An attacker could craft a script and trick the user into clicking it. When a victim who is registered on the portal clicks on such link, confidentiality and integrity of their web browser session could be compromised.	5.4	More Details
CVE-2024-20477	A vulnerability in a specific REST API endpoint of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to upload or delete files on an affected device. This vulnerability exists because of missing authorization controls on the affected REST API endpoint. An attacker could exploit this vulnerability by sending crafted API requests to the affected endpoint. A successful exploit could allow the attacker to upload files into a specific container or delete files from a specific folder within that container. This vulnerability only affects a specific REST API endpoint and does not affect the web-based management interface.	5.4	More Details
CVE-2024-41587	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6.	5.4	More Details
CVE-2024-41515	A reflected cross-site scripting (XSS) vulnerability in "ccHandlerResource.ashx" in CADClick <= 1.11.0 allows remote attackers to inject arbitrary web script or HTML via the "res_url" parameter.	5.4	More Details
CVE-2024-20442	A vulnerability in the REST API endpoints of Cisco Nexus Dashboard could allow an authenticated, low-privileged, remote attacker to perform limited Administrator actions on an affected device. This vulnerability is due to insufficient authorization controls on some REST API endpoints. An attacker could exploit this vulnerability by sending crafted API requests to an affected endpoint. A successful exploit could allow the attacker to perform limited Administrator functions such as viewing portions of the web UI, generating config only or full backup files, and deleting tech support files. This vulnerability only affects a subset of REST API endpoints and does not affect the web-based management interface.	5.4	More Details
CVE-2024-33210	A cross-site scripting (XSS) vulnerability has been identified in Flatpress 1.3. This vulnerability allows an attacker to inject malicious scripts into web pages viewed by other users.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9021	In the process of testing the Relevanssi WordPress plugin before 4.23.1, a vulnerability was found that allows you to implement Stored XSS on behalf of the Contributor+ by embedding malicious script, which entails account takeover backdoor	5.4	More Details
CVE-2024-41516	A Reflected cross-site scripting (XSS) vulnerability in "ccHandler.aspx" CADClick <= 1.11.0 allows remote attackers to inject arbitrary web script or HTML via the "bomid" parameter.	5.4	More Details
CVE-2024-8254	The Email Subscribers by Icegram Express – Email Marketing, Newsletters, Automation for WordPress & WooCommerce plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 5.7.34. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes.	5.4	More Details
CVE-2024-38036	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim’s browser.	5.4	More Details
CVE-2024-9440	Slim Select 2.0 versions through 2.9.0 are affected by a potential cross-site scripting vulnerability. In select.ts:createOption(), the text variable from the user-provided Options object is assigned to an innerHTML without sanitation. Software that depends on this library to dynamically generate lists using unsanitized user-provided input may be vulnerable to cross-site scripting, resulting in attacker executed JavaScript. At this time, no patch is available.	5.4	More Details
CVE-2024-38039	There is an HTML injection vulnerability in Esri Portal for ArcGIS versions 11.0 and below that may allow a remote, authenticated attacker to create a crafted link which when clicked could render arbitrary HTML in the victim’s browser (no stateful change made or customer data rendered).	5.4	More Details
CVE-2024-45278	SAP Commerce Backoffice does not sufficiently encode user controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker can cause limited impact on confidentiality and integrity of the application.	5.4	More Details
CVE-2024-41513	A reflected cross-site scripting (XSS) vulnerability in "Artikel.aspx" in CADClick v1.11.0 and before allows remote attackers to inject arbitrary web script or HTML via the "searchindex" parameter.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45292	PHPSpreadsheet is a pure PHP library for reading and writing spreadsheet files. `\PhpOffice\PhpSpreadsheet\Writer\Html` does not sanitize "javascript:" URLs from hyperlink `href` attributes, resulting in a Cross-Site Scripting vulnerability. This issue has been addressed in release versions 1.29.2, 2.1.1, and 2.3.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2024-46409	A stored cross-site scripting (XSS) vulnerability in SeedDMS v6.0.28 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Name parameter in the Calendar page.	5.4	More Details
CVE-2024-47618	Sulu is a PHP content management system. Sulu is vulnerable against XSS whereas a low privileged user with access to the “Media” section can upload an SVG file with a malicious payload. Once uploaded and accessed, the malicious javascript will be executed on the victims’ (other users including admins) browsers. This issue is fixed in 2.6.5.	5.4	More Details
CVE-2024-41514	A reflected cross-site scripting (XSS) vulnerability in "PrevPgGroup.aspx" in CADClick v1.11.0 and before allows remote attackers to inject arbitrary web script or HTML via the "wer" parameter.	5.4	More Details
CVE-2024-45153	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-2024-8520	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.8.6. This is due to missing or incorrect nonce validation on the admin_init or user_action_hook function. This makes it possible for unauthenticated attackers to modify a users membership status via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.3	More Details
CVE-2024-9410	Ada.cx's Sentry configuration allowed for blind server-side request forgeries (SSRF) through the use of a data scraping endpoint.	5.3	More Details
CVE-2024-47855	util/JSONTokener.java in JSON-lib before 3.1.0 mishandles an unbalanced comment string.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45231	An issue was discovered in Django v5.1.1, v5.0.9, and v4.2.16. The django.contrib.auth.forms.PasswordResetForm class, when used in a view implementing password reset flows, allows remote attackers to enumerate user e-mail addresses by sending password reset requests and observing the outcome (only when e-mail sending is consistently failing).	5.3	More Details
CVE-2022-4534	The Limit Login Attempts (Spam Protection) plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 5.3. This is due to insufficient restrictions on where the IP Address information is being retrieved for request logging and login restrictions. Attackers can supply the X-Forwarded-For header with with a different IP Address that will be logged and can be used to bypass settings that may have blocked out an IP address or country from logging in.	5.3	More Details
CVE-2024-34663	Integer overflow in libSEF.quram.so prior to SMR Oct-2024 Release 1 allows local attackers to write out-of-bounds memory.	5.3	More Details
CVE-2024-9621	A vulnerability was found in Quarkus CXF. Passwords and other secrets may appear in the application log in spite of the user configuring them to be hidden. This issue requires some special configuration to be vulnerable, such as SOAP logging enabled, application set client, and endpoint logging properties, and the attacker must have access to the application log.	5.3	More Details
CVE-2024-45297	Discourse is an open source platform for community discussion. Users can see topics with a hidden tag if they know the label/name of that tag. This issue has been patched in the latest stable, beta and tests-passed version of Discourse. All users area are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2024-47344	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in StylemixThemes uListing.This issue affects uListing: from n/a through 2.1.5.	5.3	More Details
CVE-2024-9622	A vulnerability was found in the resteasy-netty4 library arising from improper handling of HTTP requests using smuggling techniques. When an HTTP smuggling request with an ASCII control character is sent, it causes the Netty HttpObjectDecoder to transition into a BAD_MESSAGE state. As a result, any subsequent legitimate requests on the same connection are ignored, leading to client timeouts, which may impact systems using load balancers and expose them to risk.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47913	An issue was discovered in the AbuseFilter extension for MediaWiki before 1.39.9, 1.40.x and 1.41.x before 1.41.3, and 1.42.x before 1.42.2. An API caller can match a filter condition against AbuseFilter logs even if the caller is not authorized to view the log details for the filter.	5.3	More Details
CVE-2024-47563	A vulnerability has been identified in Siemens SINEC Security Monitor (All versions < V4.9.0). The affected application does not properly validate a file path that is supplied to an endpoint intended to create CSR files. This could allow an unauthenticated remote attacker to create files in writable directories outside the intended location and thus compromise integrity of files in those writable directories.	5.3	More Details
CVE-2024-8508	NLnet Labs Unbound up to and including version 1.21.0 contains a vulnerability when handling replies with very large RRsets that it needs to perform name compression for. Malicious upstreams responses with very large RRsets can cause Unbound to spend a considerable time applying name compression to downstream replies. This can lead to degraded performance and eventually denial of service in well orchestrated attacks. The vulnerability can be exploited by a malicious actor querying Unbound for the specially crafted contents of a malicious zone with very large RRsets. Before Unbound replies to the query it will try to apply name compression which was an unbounded operation that could lock the CPU until the whole packet was complete. Unbound version 1.21.1 introduces a hard limit on the number of name compression calculations it is willing to do per packet. Packets that need more compression will result in semi-compressed packets or truncated packets, even on TCP for huge messages, to avoid locking the CPU for long. This change should not affect normal DNS traffic.	5.3	More Details
CVE-2024-47211	In OpenStack Ironic before 21.4.4, 22.x and 23.x before 23.0.3, 23.x and 24.x before 24.1.3, and 25.x and 26.x before 26.1.0, there is a lack of checksum validation of supplied image_source URLs when configured to convert images to a raw format for streaming.	5.3	More Details
CVE-2024-9620	A flaw was found in Event-Driven Automation (EDA) in Ansible Automation Platform (AAP), which lacks encryption of sensitive information. An attacker with network access could exploit this vulnerability by sniffing the plaintext data transmitted between the EDA and AAP. An attacker with system access could exploit this vulnerability by reading the plaintext data stored in EDA and AAP databases.	5.3	More Details
CVE-2024-46887	The web server of affected devices do not properly authenticate user request to the '/ClientArea/RuntimeInfoData.mwsl' endpoint. This could allow an unauthenticated remote attacker to gain knowledge about current actual and configured maximum cycle times as well as about configured maximum communication load.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9423	Certain HP LaserJet printers may potentially experience a denial of service when a user sends a raw JPEG file to the printer. The printer displays a “JPEG Unsupported” message which may not clear, potentially blocking queued print jobs.	5.3	More Details
CVE-2024-47356	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Catch Themes Create allows Stored XSS.This issue affects Create: from n/a through 2.9.1.	5.1	More Details
CVE-2024-47313	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Catch Themes Catch Base allows Stored XSS.This issue affects Catch Base: from n/a through 3.4.6.	5.1	More Details
CVE-2024-47973	In some Solidigm DC Products, a defect in device overprovisioning may provide information disclosure to an attacker.	5.1	More Details
CVE-2024-44010	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Catch Themes Full frame allows Stored XSS.This issue affects Full frame: from n/a through 2.7.2.	5.1	More Details
CVE-2024-9484	An null-pointer-derefrence in the engine module in AVG/Avast Antivirus signature <24092400 released on 24/Sep/2024 on MacOS allows a malformed xar file to crash the application during file processing.	5.1	More Details
CVE-2024-9483	A null-pointer-dereference in the signature verification module in AVG/Avast Antivirus signature <24092400 released on 24/Sep/2024 on MacOS may allow a malformed xar file to crash the application during processing.	5.1	More Details
CVE-2024-9482	An out-of-bounds write in the engine module in AVG/Avast Antivirus signature <24092400 released on 24/Sep/2024 on MacOS allows a malformed Mach-O file to crash the application during file processing.	5.1	More Details
CVE-2024-9481	An out-of-bounds write in the engine module in AVG/Avast Antivirus signature <24092400 released on 24/Sep/2024 on MacOS allows a malformed eml file to crash the application during file processing.	5.1	More Details
CVE-2024-43520	Windows Kernel Denial of Service Vulnerability	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36814	An arbitrary file read vulnerability in Adguard Home before v0.107.52 allows authenticated attackers to access arbitrary files as root on the underlying Operating System via placing a crafted file into a readable directory.	4.9	More Details
CVE-2024-45894	BlueCMS 1.6 suffers from Arbitrary File Deletion via the file_name parameter in an /admin/database.php?act=del request.	4.9	More Details
CVE-2024-47948	In JetBrains TeamCity before 2024.07.3 path traversal leading to information disclosure was possible via server backups	4.9	More Details
CVE-2024-47949	In JetBrains TeamCity before 2024.07.3 path traversal allowed backup file write to arbitrary location	4.9	More Details
CVE-2024-9528	The Contact Form Plugin by Fluent Forms for Quiz, Survey, and Drag & Drop WP Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via form label fields in all versions up to, and including, 5.1.19 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with access to edit forms (administrator by default), to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.9	More Details
CVE-2024-20102	In wlan driver, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08998892; Issue ID: MSV-1601.	4.9	More Details
CVE-2024-9146	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in James Low CSS JS Files allows Path Traversal.This issue affects CSS JS Files: from n/a through 1.5.0.	4.9	More Details
CVE-2024-47840	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Wikimedia Foundation Mediawiki - Apex skin allows Stored XSS.This issue affects Mediawiki - Apex skin: from 1.39.X before 1.39.9, from 1.41.X before 1.41.3, from 1.42.X before 1.42.2.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25702	There is a stored Cross-site Scripting vulnerability in Esri Portal for ArcGIS Enterprise Sites versions 10.8.1 – 11.1 that may allow a remote, authenticated attacker to create a crafted link that is stored in the site configuration which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high. The attack could disclose a privileged token which may result in the attacker gaining full control of the Portal.	4.8	More Details
CVE-2024-45964	Zenario 9.7.61188 is vulnerable to Cross Site Scripting (XSS) in the Image library via the "Organizer tags" field.	4.8	More Details
CVE-2024-43456	Windows Remote Desktop Services Tampering Vulnerability	4.8	More Details
CVE-2024-25694	There is a stored Cross-site Scripting vulnerability in Esri Portal for ArcGIS Enterprise versions 10.8.1 – 10.9.1 that may allow a remote, authenticated attacker to create a crafted link that is stored in the Layer Showcase application configuration which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high. The attack could disclose a privileged token which may result in the attacker gaining full control of the Portal.	4.8	More Details
CVE-2024-46410	PublicCMS V4.0.202406.d was discovered to contain a cross-site scripting (XSS) vulnerability via a crafted script to the Category Managment feature	4.8	More Details
CVE-2024-8983	Custom Twitter Feeds WordPress plugin before 2.2.3 is not filtering some of its settings allowing high privilege users to inject scripts.	4.8	More Details
CVE-2024-45932	Krayin CRM v1.3.0 is vulnerable to Cross Site Scripting (XSS) via the organization name field in /admin/contacts/organizations/edit/2.	4.8	More Details
CVE-2024-45960	Zenario 9.7.61188 allows authenticated admin users to upload PDF files containing malicious code into the target system. If the PDF file is accessed through the website, it can trigger a Cross Site Scripting (XSS) attack.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25701	There is a stored Cross-site Scripting vulnerability in Esri Portal for ArcGIS Enterprise Experience Builder versions 10.8.1 – 11.1 that may allow a remote, authenticated attacker to create a crafted link that is stored in the Experience Builder Embed widget which when loaded could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high. The attack could disclose a privileged token which may result in the attacker gaining full control of the Portal.	4.8	More Details
CVE-2024-25707	There is a reflected cross site scripting in Esri Portal for ArcGIS 11.1 and below on Windows and Linux x64 allows a remote authenticated attacker with administrative access to supply a crafted string which could potentially execute arbitrary JavaScript code in the their own browser (Self XSS). A user cannot be phished into clicking a link to execute code.	4.8	More Details
CVE-2024-46886	The web server of affected devices does not properly validate input that is used for a user redirection. This could allow an attacker to make the server redirect the legitimate user to an attacker-chosen URL. For a successful exploit, the legitimate user must actively click on an attacker-crafted link.	4.7	More Details
CVE-2024-45962	October 3.6.30 allows an authenticated admin account to upload a PDF file containing malicious JavaScript into the target system. If the file is accessed through the website, it could lead to a Cross-Site Scripting (XSS) attack or execute arbitrary code via a crafted JavaScript to the target.	4.7	More Details
CVE-2024-45965	Contao 5.4.1 allows an authenticated admin account to upload a SVG file containing malicious javascript code into the target system. If the file is accessed through the website, it could lead to a Cross-Site Scripting (XSS) attack or execute arbitrary code via a crafted javascript to the target.	4.7	More Details
CVE-2024-41584	DrayTek Vigor3910 devices through 4.3.2.6 are vulnerable to reflected XSS by authenticated users, caused by missing validation of the sFormAuthStr parameter.	4.7	More Details
CVE-2024-41583	DrayTek Vigor3910 devices through 4.3.2.6 are vulnerable to stored Cross Site Scripting (XSS) by authenticated users due to poor sanitization of the router name.	4.7	More Details
CVE-2024-9266	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Express. This vulnerability affects the use of the Express Response object. This issue impacts Express: from 3.4.5 before 4.0.0.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47646	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Payflex Payflex Payment Gateway.This issue affects Payflex Payment Gateway: from n/a through 2.6.1.	4.7	More Details
CVE-2024-8499	The Checkout Field Editor (Checkout Manager) for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘render_review_request_notice’ function in all versions up to, and including, 2.0.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	4.7	More Details
CVE-2024-8149	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 11.1 and 11.2 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim’s browser.	4.6	More Details
CVE-2024-21530	Versions of the package cocoon before 0.4.0 are vulnerable to Reusing a Nonce, Key Pair in Encryption when the encrypt, wrap, and dump functions are sequentially called. An attacker can generate the same ciphertext by creating a new encrypted message with the same cocoon object. **Note:** The issue does NOT affect objects created with Cocoon::new which utilizes ThreadRng.	4.5	More Details
CVE-2024-20093	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1699.	4.4	More Details
CVE-2024-9306	The WP Booking Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 10.6 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. In addition, site administrators have the option to grant lower-level users with access to manage the plugin's settings which may extend this vulnerability to those users.	4.4	More Details
CVE-2024-31227	Redis is an open source, in-memory database that persists on disk. An authenticated with sufficient privileges may create a malformed ACL selector which, when accessed, triggers a server panic and subsequent denial of service. The problem exists in Redis 7 prior to versions 7.2.6 and 7.4.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47967	Improper resource initialization handling in firmware of some Solidigm DC Products may allow an attacker to potentially enable denial of service.	4.4	More Details
CVE-2024-47974	Race condition during resource shutdown in some Solidigm DC Products may allow an attacker to potentially enable denial of service.	4.4	More Details
CVE-2024-47968	Improper resource shutdown in middle of certain operations on some Solidigm DC Products may allow an attacker to potentially enable denial of service.	4.4	More Details
CVE-2024-39831	in OpenHarmony v4.1.0 allow a local attacker with high privileges arbitrary code execution in pre-installed apps through use after free.	4.4	More Details
CVE-2024-20095	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996894; Issue ID: MSV-1636.	4.4	More Details
CVE-2024-20091	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1701.	4.4	More Details
CVE-2024-20096	In m4u, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08996900; Issue ID: MSV-1635.	4.4	More Details
CVE-2024-20097	In vdec, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09028313; Issue ID: MSV-1630.	4.4	More Details
CVE-2024-8488	The Survey Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Survey fields in all versions up to, and including, 4.9.7 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.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44207	This issue was addressed with improved checks. This issue is fixed in iOS 18.0.1 and iPadOS 18.0.1. Audio messages in Messages may be able to capture a few seconds of audio before the microphone indicator is activated.	4.3	More Details
CVE-2024-45277	The SAP HANA Node.js client package versions from 2.0.0 before 2.21.31 is impacted by Prototype Pollution vulnerability allowing an attacker to add arbitrary properties to global object prototypes. This is due to improper user input sanitation when using the nestTables feature causing low impact on the availability of the application. This has no impact on Confidentiality and Integrity.	4.3	More Details
CVE-2024-47803	Jenkins 2.478 and earlier, LTS 2.462.2 and earlier does not redact multi-line secret values in error messages generated for form submissions involving the `secretTextarea` form field.	4.3	More Details
CVE-2024-47161	In JetBrains TeamCity before 2024.07.3 password could be exposed via Sonar runner REST API	4.3	More Details
CVE-2024-47804	If an attempt is made to create an item of a type prohibited by `ACL#hasCreatePermission2` or `TopLevelItemDescriptor#isApplicableIn(ItemGroup)` through the Jenkins CLI or the REST API and either of these checks fail, Jenkins 2.478 and earlier, LTS 2.462.2 and earlier creates the item in memory, only deleting it from disk, allowing attackers with Item/Configure permission to save the item to persist it, effectively bypassing the item creation restriction.	4.3	More Details
CVE-2024-8431	The Photo Gallery, Images, Slider in Rbs Image Gallery plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the ajaxGetGalleryJson() function in all versions up to, and including, 3.2.21. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve private post titles.	4.3	More Details
CVE-2024-47554	Uncontrolled Resource Consumption vulnerability in Apache Commons IO. The org.apache.commons.io.input.XmlStreamReader class may excessively consume CPU resources when processing maliciously crafted input. This issue affects Apache Commons IO: from 2.0 before 2.14.0. Users are recommended to upgrade to version 2.14.0 or later, which fixes the issue.	4.3	More Details
CVE-2024-42504	A security vulnerability in HPE IceWall Agent products could be exploited remotely to cause a Cross-Site Request Forgery (CSRF) in the login flow.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45282	Fields which are in 'read only' state in Bank Statement Draft in Manage Bank Statements application, could be modified by MERGE method. The property of an OData entity representing assumably immutable method is not protected against external modifications leading to integrity violations. Confidentiality and Availability are not impacted.	4.3	More Details
CVE-2024-45250	ZKteco – CWE 200 Exposure of Sensitive Information to an Unauthorized Actor	4.3	More Details
CVE-2024-47316	Authorization Bypass Through User-Controlled Key vulnerability in Salon Booking System Salon booking system.This issue affects Salon booking system: from n/a through 10.9.	4.3	More Details
CVE-2024-47565	A vulnerability has been identified in Siemens SINEC Security Monitor (All versions < V4.9.0). The affected application does not properly validate that user input complies with a list of allowed values. This could allow an authenticated remote attacker to compromise the integrity of the configuration of the affected application.	4.3	More Details
CVE-2024-47822	Directus is a real-time API and App dashboard for managing SQL database content. Access tokens from query strings are not redacted and are potentially exposed in system logs which may be persisted. The access token in `req.query` is not redacted when the `LOG_STYLE` is set to `raw`. If these logs are not properly sanitized or protected, an attacker with access to it can potentially gain administrative control, leading to unauthorized data access and manipulation. This impacts systems where the `LOG_STYLE` is set to `raw`. The `access_token` in the query could potentially be a long-lived static token. Users with impacted systems should rotate their static tokens if they were provided using query string. This vulnerability has been patched in release version 10.13.2 and subsequent releases as well. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.2	More Details
CVE-2024-34664	Improper check for exception conditions in Knox Guard prior to SMR Oct-2024 Release 1 allows physical attackers to bypass Knox Guard in a multi-user environment.	4.1	More Details
CVE-2024-34670	Use of implicit intent for sensitive communication in Sound Assistant prior to version 6.1.0.9 allows local attackers to get sensitive information.	4.0	More Details
CVE-2024-47972	Improper resource management in firmware of some Solidigm DC Products may allow an attacker to potentially control the performance of the resource.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41511	A Path Traversal (Local File Inclusion) vulnerability in "BinaryFileRedirector.ashx" in CADClick v1.11.0 and before allows remote attackers to retrieve arbitrary local files via the "path" parameter.	3.9	More Details
CVE-2024-47814	Vim is an open source, command line text editor. A use-after-free was found in Vim < 9.1.0764. When closing a buffer (visible in a window) a BufWinLeave auto command can cause an use-after-free if this auto command happens to re-open the same buffer in a new split window. Impact is low since the user must have intentionally set up such a strange auto command and run some buffer unload commands. However this may lead to a crash. This issue has been addressed in version 9.1.0764 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	3.9	More Details
CVE-2024-9513	A vulnerability was found in Netadmin Software NetAdmin IAM up to 3.5 and classified as problematic. Affected by this issue is some unknown functionality of the file /controller/api/Answer/ReturnUserQuestionsFilled of the component HTTP POST Request Handler. The manipulation of the argument username leads to information exposure through discrepancy. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure is planning to release a fix in mid-October 2024.	3.7	More Details
CVE-2024-9554	A vulnerability classified as problematic was found in Sovell Smart Canteen System up to 3.0.7303.30513. Affected by this vulnerability is the function Check_ET_CheckPwdz201 of the file suanfa.py of the component Password Reset Handler. The manipulation leads to authorization bypass. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2024-47951	In JetBrains TeamCity before 2024.07.3 stored XSS was possible via server global settings	3.5	More Details
CVE-2024-47612	DataDump is a MediaWiki extension that provides dumps of wikis. Several interface messages are unescaped (more specifically, (datadump-table-column-queued), (datadump-table-column-in-progress), (datadump-table-column-completed), (datadump-table-column-failed)). If these messages are edited (which requires the (editinterface) right by default), anyone who can view Special:DataDump (which requires the (view-dump) right by default) can be XSSed. This vulnerability is fixed with 601688ee8e8808a23b102fa305b178f27cbd226d.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47950	In JetBrains TeamCity before 2024.07.3 stored XSS was possible in Backup configuration settings	3.5	More Details
CVE-2024-43696	in OpenHarmony v4.1.0 and prior versions allow a local attacker cause DOS by memory leak.	3.3	More Details
CVE-2024-0125	NVIDIA CUDA Toolkit for Windows and Linux contains a vulnerability in the nvdisam command line tool, where a user can cause a NULL pointer dereference by running nvdisasm on a malformed ELF file. A successful exploit of this vulnerability might lead to a limited denial of service.	3.3	More Details
CVE-2024-33506	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in FortiManager 7.4.2 and below, 7.2.5 and below, 7.0.12 and below allows a remote authenticated attacker assigned to an Administrative Domain (ADOM) to access device summary of unauthorized ADOMs via crafted HTTP requests.	3.3	More Details
CVE-2024-24122	A remote code execution vulnerability in the project management of Wanxing Technology's Yitu project which allows an attacker to use the exp.adpx file as a zip compressed file to construct a special file name, which can be used to decompress the project file into the system startup folder, restart the system, and automatically execute the constructed attack script.	3.3	More Details
CVE-2024-8518	CWE-20: Improper Input Validation vulnerability exists that could cause a crash of the Zelio Soft 2 application when a specially crafted project file is loaded by an application user.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45476	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0016), Tecnomatix Plant Simulation V2404 (All versions < V2404.0005). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted WRL files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	3.3	More Details
CVE-2024-0124	NVIDIA CUDA Toolkit for Windows and Linux contains a vulnerability in the nvdisam command line tool, where a user can cause nvdisasm to read freed memory by running it on a malformed ELF file. A successful exploit of this vulnerability might lead to a limited denial of service.	3.3	More Details
CVE-2024-0123	NVIDIA CUDA toolkit for Windows and Linux contains a vulnerability in the nvdisasm command line tool where an attacker may cause an improper validation in input issue by tricking the user into running nvdisasm on a malicious ELF file. A successful exploit of this vulnerability may lead to denial of service.	3.3	More Details
CVE-2024-45382	in OpenHarmony v4.1.0 and prior versions allow a local attacker cause DOS through out-of-bounds write.	3.3	More Details
CVE-2024-34671	Use of implicit intent for sensitive communication in translation훍in Samsung Internet prior to version 26.0.3.1 allows local attackers to get sensitive information. User interaction is required for triggering this vulnerability.	3.3	More Details
CVE-2024-9026	In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, when using PHP-FPM SAPI and it is configured to catch workers output through catch_workers_output = yes, it may be possible to pollute the final log or remove up to 4 characters from the log messages by manipulating log message content. Additionally, if PHP-FPM is configured to use syslog output, it may be possible to further remove log data using the same vulnerability.	3.3	More Details
CVE-2024-43697	in OpenHarmony v4.1.0 and prior versions allow a local attacker cause DOS through improper input.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47780	TYPO3 is a free and open source Content Management Framework. Backend users could see items in the backend page tree without having access if the mounts pointed to pages restricted for their user/group, or if no mounts were configured but the pages allowed access to "everybody." However, affected users could not manipulate these pages. Users are advised to update to TYPO3 versions 10.4.46 ELTS, 11.5.40 LTS, 12.4.21 LTS, 13.3.1 that fix the problem described. There are no known workarounds for this vulnerability.	3.1	More Details
CVE-2024-8925	In PHP versions 8.1.* before 8.1.30, 8.2.* before 8.2.24, 8.3.* before 8.3.12, erroneous parsing of multipart form data contained in an HTTP POST request could lead to legitimate data not being processed. This could lead to malicious attacker able to control part of the submitted data being able to exclude portion of other data, potentially leading to erroneous application behavior.	3.1	More Details
CVE-2024-27457	Improper check for unusual or exceptional conditions in Intel(R) TDX Module firmware before version 1.5.06 may allow a privileged user to potentially enable information disclosure via local access.	2.5	More Details
CVE-2024-7206	SSL Pinning Bypass in eWeLink Some hardware products allows local ATTACKER to Decrypt TLS communication and Extract secrets to clone the device via Flash the modified firmware	N/A	More Details
CVE-2024-9174	Stored HTML Injection in Social Module in M-Files Hubshare before version 5.0.8.6 allows authenticated user to spoof UI	N/A	More Details
CVE-2024-9412	An improper authorization vulnerability exists in the Rockwell Automation affected products that could allow an unauthorized user to sign in. While removal of all role mappings is unlikely, it could occur in the case of unexpected or accidental removal by the administrator. If exploited, an unauthorized user could access data they previously but should no longer have access to.	N/A	More Details
CVE-2024-9333	Permissions bypass in M-Files Connector for Copilot before version 24.9.3 allows authenticated user to access limited amount of documents via incorrect access control list calculation	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47823	Livewire is a full-stack framework for Laravel that allows for dynamic UI components without leaving PHP. In livewire/livewire prior to `2.12.7` and `v3.5.2`, the file extension of an uploaded file is guessed based on the MIME type. As a result, the actual file extension from the file name is not validated. An attacker can therefore bypass the validation by uploading a file with a valid MIME type (e.g., `image/png`) and a ".php" file extension. If the following criteria are met, the attacker can carry out an RCE attack: 1. Filename is composed of the original file name using `$file->getClientOriginalName()`. 2. Files stored directly on your server in a public storage disk. 3. Webserver is configured to execute ".php" files. This issue has been addressed in release versions `2.12.7` and `3.5.2`. All users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2024-47611	XZ Utils provide a general-purpose data-compression library plus command-line tools. When built for native Windows (MinGW-w64 or MSVC), the command line tools from XZ Utils 5.6.2 and older have a command line argument injection vulnerability. If a command line contains Unicode characters (for example, filenames) that don't exist in the current legacy code page, the characters are converted to similar-looking characters with best-fit mapping. Some best-fit mappings result in ASCII characters that change the meaning of the command line, which can be exploited with malicious filenames to do argument injection or directory traversal attacks. This vulnerability is fixed in 5.6.3. Command line tools built for Cygwin or MSYS2 are unaffected. liblzma is unaffected.	N/A	More Details
CVE-2024-47848	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in The Wikimedia Foundation Mediawiki - PageTriage allows Authentication Bypass.This issue affects Mediawiki - PageTriage: from 1.39.X before 1.39.9, from 1.41.X before 1.41.3, from 1.42.X before 1.42.2.	N/A	More Details
CVE-2024-47095	Cross Site Scripting vulnerability in Follet School Solutions Destiny before v22.0.1 AU1 allows a remote attacker to run arbitrary client-side code via the expiredSupportMessage parameter of handleloginform.do.	N/A	More Details
CVE-2024-6360	Incorrect Permission Assignment for Critical Resource vulnerability in OpenText™ Vertica could allow Privilege Abuse and result in unauthorized access or privileges to Vertica agent apikey. This issue affects Vertica: from 10.0 through 10.X, from 11.0 through 11.X, from 12.0 through 12.X, from 23.0 through 23.X, from 24.0 through 24.X.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47764	cookie is a basic HTTP cookie parser and serializer for HTTP servers. The cookie name could be used to set other fields of the cookie, resulting in an unexpected cookie value. A similar escape can be used for path and domain, which could be abused to alter other fields of the cookie. Upgrade to 0.7.0, which updates the validation for name, path, and domain.	N/A	More Details
CVE-2024-8626	Due to a memory leak, a denial-of-service vulnerability exists in the Rockwell Automation affected products. A malicious actor could exploit this vulnerability by performing multiple actions on certain web pages of the product causing the affected products to become fully unavailable and require a power cycle to recover.	N/A	More Details
CVE-2024-47790	** UNSUPPORTED WHEN ASSIGNED ** This vulnerability exists in D3D Security IP Camera D8801 due to usage of insecure Real-Time Streaming Protocol (RTSP) version for live video streaming. A remote attacker could exploit this vulnerability by crafting a RTSP packet leading to unauthorized access to live feed of the targeted device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	N/A	More Details
CVE-2024-47789	** UNSUPPORTED WHEN ASSIGNED ** This vulnerability exists in D3D Security IP Camera D8801 due to usage of weak authentication scheme of the HTTP header protocol where authorization tag contain a Base-64 encoded username and password. A remote attacker could exploit this vulnerability by crafting a HTTP packet leading to exposure of user credentials of the targeted device. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	N/A	More Details
CVE-2024-41987	The TEM Opera Plus FM Family Transmitter application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.	N/A	More Details
CVE-2024-41988	TEM Opera Plus FM Family Transmitter allows access to an unprotected endpoint that allows MPFS File System binary image upload without authentication. This file system serves as the basis for the HTTP2 web server module but is also used by the SNMP module and is available to other applications that require basic read-only storage capabilities. This can be exploited to overwrite the flash program memory that holds the web server's main interfaces and execute arbitrary code.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9124	A denial-of-service vulnerability exists in the Rockwell Automation PowerFlex® 600T. If the device is overloaded with requests, it will become unavailable. The device may require a power cycle to recover it if it does not re-establish a connection after it stops receiving requests.	N/A	More Details