SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 19 June 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-2024-3922	The Dokan Pro plugin for WordPress is vulnerable to SQL Injection via the 'code' parameter in all versions up to, and including, 3.10.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	10.0	More Details
CVE-2024-30299	Adobe Framemaker Publishing Server versions 2020.3, 2022.2 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction.	10.0	More Details
CVE-2024-37902	DeepJavaLibrary(DJL) is an Engine-Agnostic Deep Learning Framework in Java. DJL versions 0.1.0 through 0.27.0 do not prevent absolute path archived artifacts from inserting archived files directly into the system, overwriting system files. This is fixed in DJL 0.28.0 and patched in DJL Large Model Inference containers version 0.27.0. Users are advised to upgrade.	10.0	More Details
CVE-2024-3105	The Woody code snippets – Insert Header Footer Code, AdSense Ads plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.5.0 via the 'insert_php' shortcode. This is due to the plugin not restricting the usage of the functionality to high level authorized users. This makes it possible for authenticated attackers, with contributor-level access and above, to execute code on the server.	9.9	More Details
CVE-2024-37831	Itsourcecode Payroll Management System 1.0 is vulnerable to SQL Injection in payroll_items.php via the ID parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38441	Netatalk before 3.2.1 has an off-by-one error and resultant heap-based buffer overflow because of setting ibuf[len] to '\0' in FPMapName in afp_mapname in etc/afpd/directory.c. 2.4.1 and 3.1.19 are also fixed versions.	9.8	More Details
CVE-2024-38439	Netatalk before 3.2.1 has an off-by-one error and resultant heap-based buffer overflow because of setting ibuf[PASSWDLEN] to '\0' in FPLoginExt in login in etc/uams/uams_pam.c. 2.4.1 and 3.1.19 are also fixed versions.	9.8	More Details
CVE-2024-38395	In iTerm2 before 3.5.2, the "Terminal may report window title" setting is not honored, and thus remote code execution might occur but "is not trivially exploitable."	9.8	More Details
CVE-2024-4258	The Video Gallery – YouTube Playlist, Channel Gallery by YotuWP plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.3.13 via the settings parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	9.8	More Details
CVE-2024-5871	The WooCommerce - Social Login plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.6.2 via deserialization of untrusted input from the 'woo_slg_verify' vulnerable parameter. This makes it possible for unauthenticated attackers 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.	9.8	More Details
CVE-2024-4898	The InstaWP Connect – 1-click WP Staging & Migration plugin for WordPress is vulnerable to arbitrary option updates due to a missing authorization checks on the REST API calls in all versions up to, and including, 0.1.0.38. This makes it possible for unauthenticated attackers to connect the site to InstaWP API, edit arbitrary site options and create administrator accounts.	9.8	More Details
CVE-2024-38466	Shenzhen Guoxin Synthesis image system before 8.3.0 has a 123456Qw default password.	9.8	More Details
CVE-2024-33375	LB-LINK BL-W1210M v2.0 was discovered to store user credentials in plaintext within the router's firmware.	9.8	More Details
CVE-2024-33374	Incorrect access control in the UART/Serial interface on the LB-LINK BL-W1210M v2.0 router allows attackers to access the root terminal without authentication.	9.8	More Details
CVE-2024-5671	Insecure Deserialization in some workflows of the IPS Manager allows unauthenticated remote attackers to perform arbitrary code execution and access to the vulnerable Trellix IPS Manager.	9.8	More Details
CVE-2024-37637	TOTOLINK A3700R V9.1.2u.6165_20211012 was discovered to contain a stack overflow via ssid5g in the function setWizardCfg.	9.8	More Details
CVE-2024-3912	Certain models of ASUS routers have an arbitrary firmware upload vulnerability. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary system commands on the device.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5577	The Where I Was, Where I Will Be plugin for WordPress is vulnerable to Remote File Inclusion in version <= 1.1.1 via the WIW_HEADER parameter of the /system/include/include_user.php file. This makes it possible for unauthenticated attackers to include and execute arbitrary files hosted on external servers, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution. This requires allow_url_include to be set to true in order to exploit, which is not commonly enabled.	9.8	More Details
CVE-2024-38462	iRODS before 4.3.2 provides an msiSendMail function with a problematic dependency on the mail binary, such as in the mailMS.cpp#L94-L106 reference.	9.8	More Details
CVE-2024-38396	An issue was discovered in iTerm2 3.5.x before 3.5.2. Unfiltered use of an escape sequence to report a window title, in combination with the built-in tmux integration feature (enabled by default), allows an attacker to inject arbitrary code into the terminal, a different vulnerability than CVE-2024-38395.	9.8	More Details
CVE-2024-38468	Shenzhen Guoxin Synthesis image system before 8.3.0 allows unauthorized password resets via the resetPassword API.	9.8	More Details
CVE-2024-27174	Remote Command program allows an attacker to get Remote Code Execution. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	9.8	More Details
CVE-2024-5163	Improper permission settings for mobile applications (com.transsion.carlcare) may lead to user password and account security risks.	9.8	More Details
CVE-2024-6047	Certain EOL GeoVision devices fail to properly filter user input for the specific functionality. Unauthenticated remote attackers can exploit this vulnerability to inject and execute arbitrary system commands on the device.	9.8	More Details
CVE-2024-6048	Openfind's MailGates and MailAudit fail to properly filter user input when analyzing email attachments. An unauthenticated remote attacker can exploit this vulnerability to inject system commands and execute them on the remote server.	9.8	More Details
CVE-2024-6057	Improper authentication in the vault password feature in Devolutions Remote Desktop Manager 2024.1.31.0 and earlier allows an attacker that has compromised an access to an RDM instance to bypass the vault master password via the offline mode feature.	9.8	More Details
CVE-2024-36580	A Prototype Pollution issue in cdr0 sg 1.0.10 allows an attacker to execute arbitrary code.	9.8	More Details
CVE-2024-36582	alexbinary object-deep-assign 1.0.11 is vulnerable to Prototype Pollution via the extend() method of Module.deepAssign (/src/index.js)	9.8	More Details
CVE-2024-36573	almela obx before v.0.0.4 has a Prototype Pollution issue which allows arbitrary code execution via the obx/build/index.js:656), reduce (@almela/obx/build/index.js:470), Object.set (obx/build/index.js:269) component.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36575	A Prototype Pollution issue in getsetprop 1.1.0 allows an attacker to execute arbitrary code via global.accessor.	9.8	More Details
CVE-2024-36543	Incorrect access control in the Kafka Connect REST API in the STRIMZI Project 0.41.0 and earlier allows an attacker to deny the service for Kafka Mirroring, potentially mirror the topics' content to his Kafka cluster via a malicious connector (bypassing Kafka ACL if it exists), and potentially steal Kafka SASL credentials, by querying the MirrorMaker Kafka REST API.	9.8	More Details
CVE-2023-37057	An issue in JLINK Unionman Technology Co. Ltd Jlink AX1800 v.1.0 allows a remote attacker to execute arbitrary code via the router's authentication mechanism.	9.8	More Details
CVE-2023-37058	Insecure Permissions vulnerability in JLINK Unionman Technology Co. Ltd Jlink AX1800 v.1.0 allows a remote attacker to escalate privileges via a crafted command.	9.8	More Details
CVE-2024-34833	Sourcecodester Payroll Management System v1.0 is vulnerable to File Upload. Users can upload images via the "save_settings" page. An unauthenticated attacker can leverage this functionality to upload a malicious PHP file instead. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as the user running the web server.	9.8	More Details
CVE-2024-37079	vCenter Server contains a heap-overflow vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger this vulnerability by sending a specially crafted network packet potentially leading to remote code execution.	9.8	More Details
CVE-2024-1576	SQL Injection vulnerability in MegaBIP software allows attacker to obtain site administrator privileges, including access to the administration panel and the ability to change the administrator password. This issue affects MegaBIP software versions through 5.09.	9.8	More Details
CVE-2024-4936	The Canto plugin for WordPress is vulnerable to Remote File Inclusion in all versions up to, and including, 3.0.8 via the abspath parameter. This makes it possible for unauthenticated attackers to include remote files on the server, resulting in code execution. This required allow_url_include to be enabled on the target site in order to exploit.	9.8	More Details
CVE-2024-27173	Remote Command program allows an attacker to get Remote Code Execution by overwriting existing Python files containing executable code. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	9.8	More Details
CVE-2024-38295	ALCASAR before 3.6.1 allows still_connected.php remote code execution.	9.8	More Details
CVE-2024-27172	Remote Command program allows an attacker to get Remote Code Execution. As for the affected products/models/versions, see the reference URL.	9.8	More Details
CVE-2024-22441	HPE Cray Parallel Application Launch Service (PALS) is subject to an authentication bypass.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37849	A SQL Injection vulnerability in itsourcecode Billing System 1.0 allows a local attacker to execute arbitrary code in process.php via the username parameter.	9.8	More Details
CVE-2024-30300	Adobe Framemaker Publishing Server versions 2020.3, 2022.2 and earlier are affected by an Information Exposure vulnerability (CWE-200) that could lead to privilege escalation. An attacker could exploit this vulnerability to gain access to sensitive information which may include system or user privileges. Exploitation of this issue does not require user interaction.	9.8	More Details
CVE-2024-34102	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in arbitrary code execution. An attacker could exploit this vulnerability by sending a crafted XML document that references external entities. Exploitation of this issue does not require user interaction.	9.8	More Details
CVE-2024-3552	The Web Directory Free WordPress plugin before 1.7.0 does not sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection with different techniques like UNION, Time-Based and Error-Based.	9.8	More Details
CVE-2024-38294	ALCASAR before 3.6.1 allows email_registration_back.php remote code execution.	9.8	More Details
CVE-2024-37634	TOTOLINK A3700R V9.1.2u.6165_20211012 was discovered to contain a stack overflow via ssid in the function setWiFiEasyCfg.	9.8	More Details
CVE-2024-37036	CWE-787: Out-of-bounds Write vulnerability exists that could result in an authentication bypass when sending a malformed POST request and particular configuration parameters are set.	9.8	More Details
CVE-2024-36761	naga v0.14.0 was discovered to contain a stack overflow via the component /wgsl/parse/mod.rs.	9.8	More Details
CVE-2024-36265	** UNSUPPORTED WHEN ASSIGNED ** Incorrect Authorization vulnerability in Apache Submarine Server Core. This issue affects Apache Submarine Server Core: from 0.8.0. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an alternative or restrict access to the instance to trusted users. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2024-36264	** UNSUPPORTED WHEN ASSIGNED ** Improper Authentication vulnerability in Apache Submarine Commons Utils. If the user doesn't explicitly set `submarine.auth.default.secret`, a default value will be used. This issue affects Apache Submarine Commons Utils: from 0.8.0. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an alternative or restrict access to the instance to trusted users. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2024-1659	Arbitrary File Upload vulnerability in MegaBIP software allows attacker to upload any file to the server (including a PHP code file) without an authentication. This issue affects MegaBIP software versions through 5.10.	9.8	More Details
CVE-2024-1577	Remote Code Execution vulnerability in MegaBIP software allows to execute arbitrary code on the server without requiring authentication by saving crafted by the attacker PHP code to one of the website files. This issue affects MegaBIP software versions through 5.11.2.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37632	TOTOLINK A3700R V9.1.2u.6165_20211012 was discovered to contain a stack overflow via the password parameter in function loginAuth .	9.8	More Details
CVE-2024-38281	An attacker can access the maintenance console using hard coded credentials for a hidden wireless network on the device.	9.8	More Details
CVE-2024-37080	vCenter Server contains a heap-overflow vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger this vulnerability by sending a specially crafted network packet potentially leading to remote code execution.	9.8	More Details
CVE-2024-37635	TOTOLINK A3700R V9.1.2u.6165_20211012 was discovered to contain a stack overflow via ssid in the function setWiFiBasicCfg	9.8	More Details
CVE-2024-29786	In pktproc_fill_data_addr_without_bm of link_rx_pktproc.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2024-32905	In circ_read of link_device_memory_legacy.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2024-32911	There is a possible escalation of privilege due to improperly used crypto. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2024-3080	Certain ASUS router models have authentication bypass vulnerability, allowing unauthenticated remote attackers to log in the device.	9.8	More Details
CVE-2024-27145	The Toshiba printers provide several ways to upload files using the admin web interface. An attacker can remotely compromise any Toshiba printer. An attacker can overwrite any insecure files. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	9.8	More Details
CVE-2024-27144	The Toshiba printers provide several ways to upload files using the web interface without authentication. An attacker can overwrite any insecure files. And the Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. The programs can be replaced by malicious programs by any local or remote attacker. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	9.8	More Details
CVE-2024-32913	In wl_notify_rx_mgmt_frame of wl_cfg80211.c, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27143	Toshiba printers use SNMP for configuration. Using the private community, it is possible to remotely execute commands as root on the remote printer. Using this vulnerability will allow any attacker to get a root access on a remote Toshiba printer. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	9.8	More Details
CVE-2024-31777	File Upload vulnerability in openeclass v.3.15 and before allows an attacker to execute arbitrary code via a crafted file to the certbadge.php endpoint.	9.8	More Details
CVE-2024-38293	ALCASAR before 3.6.1 allows CSRF and remote code execution in activity.php.	9.6	More Details
CVE-2024-34539	Hardcoded credentials in TerraMaster TOS firmware through 5.1 allow a remote attacker to successfully login to the mail or webmail server. These credentials can also be used to login to the administration panel and to perform privileged actions.	9.4	More Details
CVE-2024-38448	htags in GNU Global through 6.6.12 allows code execution in situations where dbpath (aka -d) is untrusted, because shell metacharacters may be used.	9.1	More Details
CVE-2024-37642	TRENDnet TEW-814DAP v1_(FW1.01B01) was discovered to contain a command injection vulnerability via the ipv4_ping, ipv6_ping parameter at /formSystemCheck .	9.1	More Details
CVE-2024-36840	SQL Injection vulnerability in Boelter Blue System Management v.1.3 allows a remote attacker to execute arbitrary code and obtain sensitive information via the id parameter to news_details.php and location_details.php; and the section parameter to services.php.	9.1	More Details
CVE-2024-34108	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction, but admin privileges are required and scope is changed.	9.1	More Details
CVE-2024-2472	The LatePoint Plugin plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a missing capability check on the 'start_or_use_session_for_customer' function in all versions up to and including 4.9.9. This makes it possible for unauthenticated attackers to view other customer's cabinets, including the ability to view PII such as email addresses and to change their LatePoint user password, which may or may not be associated with a WordPress account.	9.1	More Details
CVE-2024-34451	Ghost through 5.85.1 allows remote attackers to bypass an authentication rate-limit protection mechanism by using many X-Forwarded-For headers with different values. NOTE: the vendor's position is that Ghost should be installed with a reverse proxy that allows only trusted X-Forwarded-For headers.	9.1	More Details
CVE-2024-38428	url.c in GNU Wget through 1.24.5 mishandles semicolons in the userinfo subcomponent of a URI, and thus there may be insecure behavior in which data that was supposed to be in the userinfo subcomponent is misinterpreted to be part of the host subcomponent.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0095	NVIDIA Triton Inference Server for Linux and Windows contains a vulnerability where a user can inject forged logs and executable commands by injecting arbitrary data as a new log entry. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	9.0	More Details
CVE-2024-4371	The CoDesigner WooCommerce Builder for Elementor – Customize Checkout, Shop, Email, Products & More plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 4.4.1 via deserialization of untrusted input from the recently_viewed_products cookie. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-37840	SQL injection vulnerability in processscore.php in Itsourcecode Learning Management System Project In PHP With Source Code v1.0 allows remote attackers to execute arbitrary SQL commands via the LessonID parameter.	8.8	More Details
CVE-2024-37631	TOTOLINK A3700R V9.1.2u.6165_20211012 was discovered to contain a stack overflow via the File parameter in function UploadCustomModule.	8.8	More Details
CVE-2024-5924	Dropbox Desktop Folder Sharing Mark-of-the-Web Bypass Vulnerability. This vulnerability allows remote attackers to bypass the Mark-of-the-Web protection mechanism on affected installations of Dropbox Desktop. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of shared folders. When syncing files from a shared folder belonging to an untrusted account, the Dropbox desktop application does not apply the Mark-of-the-Web to the local files. An attacker can leverage this vulnerability to execute arbitrary code in the context of the current user. Was ZDI-CAN-23991.	8.8	More Details
CVE-2024-5948	Deep Sea Electronics DSE855 Multipart Boundary Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Deep Sea Electronics DSE855 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of multipart boundaries. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-23170.	8.8	More Details
CVE-2024-5950	Deep Sea Electronics DSE855 Multipart Value Handling Stack-Based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Deep Sea Electronics DSE855 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of multipart form variables. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-23172.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37896	Gin-vue-admin is a backstage management system based on vue and gin. Gin-vue-admin <= v2.6.5 has SQL injection vulnerability. The SQL injection vulnerabilities occur when a web application allows users to input data into SQL queries without sufficiently validating or sanitizing the input. Failing to properly enforce restrictions on user input could mean that even a basic form input field can be used to inject arbitrary and potentially dangerous SQL commands. This could lead to unauthorized access to the database, data leakage, data manipulation, or even complete compromise of the database server. This vulnerability has been addressed in commit `53d033821` which has been included in release version 2.6.6. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2024-38427	In International Color Consortium DemoIccMAX before 85ce74e, a logic flaw in CIccTagXmlProfileSequenceId::ParseXml in IccXML/IccLibXML/IccTagXml.cpp results in unconditionally returning false.	8.8	More Details
CVE-2024-36597	Aegon Life v1.0 was discovered to contain a SQL injection vulnerability via the client_id parameter at clientStatus.php.	8.8	More Details
CVE-2024-38457	Xenforo before 2.2.16 allows CSRF.	8.8	More Details
CVE-2024-4845	The Icegram Express plugin for WordPress is vulnerable to SQL Injection via the 'options[list_id]' parameter in all versions up to, and including, 5.7.22 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2024-3497	Path traversal vulnerability in the web server of the Toshiba printer enables attacker to overwrite orginal files or add new ones to the printer. As for the affected products/models/versions, see the reference URL.	8.8	More Details
CVE-2024-38458	Xenforo before 2.2.16 allows code injection.	8.8	More Details
CVE-2024-24320	Directory Traversal vulnerability in Mgt-commerce CloudPanel v.2.0.0 thru v.2.4.0 allows a remote attacker to obtain sensitive information and execute arbitrary code via the service parameter of the load-logfiles function.	8.8	More Details
CVE-2024-3496	Attackers can bypass the web login authentication process to gain access to the printer's system information and upload malicious drivers to the printer. As for the affected products/models/versions, see the reference URL.	8.8	More Details
CVE-2024-32925	In dhd_prot_txstatus_process of dhd_msgbuf.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2024-37644	TRENDnet TEW-814DAP v1_(FW1.01B01) was discovered to contain a hardcoded password vulnerability in /etc/shadow.sample, which allows attackers to log in as root.	8.8	More Details
CVE-2024-37641	TRENDnet TEW-814DAP v1_(FW1.01B01) was discovered to contain a stack overflow via the submit-url parameter at /formNewSchedule	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37645	TRENDnet TEW-814DAP v1_(FW1.01B01) was discovered to contain a stack overflow vulnerability via the submit-url parameter at /formSysLog .	8.8	More Details
CVE-2024-37665	An access control issue in Wvp GB28181 Pro 2.0 allows authenticated attackers to escalate privileges to Administrator via a crafted POST request.	8.8	More Details
CVE-2024-37643	TRENDnet TEW-814DAP v1_(FW1.01B01) was discovered to contain a stack overflow vulnerability via the submit-url parameter at /formPasswordAuth .	8.8	More Details
CVE-2024-37633	TOTOLINK A3700R V9.1.2u.6165_20211012 was discovered to contain a stack overflow via ssid in the function setWiFiGuestCfg	8.8	More Details
CVE-2024-38347	CodeProjects Health Care hospital Management System v1.0 was discovered to contain a SQL injection vulnerability in the Room Information module via the id parameter.	8.8	More Details
CVE-2024-2024	The Folders Pro plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'handle_folders_file_upload' function in all versions up to, and including, 3.0.2. This makes it possible for authenticated attackers, with author 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-2024-38276	Incorrect CSRF token checks resulted in multiple CSRF risks.	8.8	More Details
CVE-2024-5995	The notification emails sent by Soar Cloud HR Portal contain a link with a embedded session. The expiration of the session is not properly configured, remaining valid for more than 7 days and can be reused.	8.8	More Details
CVE-2024-3813	The tagDiv Composer plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 4.8 via the 'td_block_title' shortcode 'block_template_id' attribute. This makes it possible for authenticated attackers, with contributor-level and above permissions, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where php file type can be uploaded and included.	8.8	More Details
CVE-2024-37821	An arbitrary file upload vulnerability in the Upload Template function of Dolibarr ERP CRM up to v19.0.1 allows attackers to execute arbitrary code via uploading a crafted .SQL file.	8.8	More Details
CVE-2024-36396	Verint - CWE-434: Unrestricted Upload of File with Dangerous Type	8.8	More Details
CVE-2024-25949	Dell OS10 Networking Switches, versions10.5.6.x, 10.5.5.x, 10.5.4.x and 10.5.3.x ,contain an improper authorization vulnerability. A remote authenticated attacker could potentially exploit this vulnerability leading to escalation of privileges.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38348	CodeProjects Health Care hospital Management System v1.0 was discovered to contain a SQL injection vulnerability in the Staff Info module via the searvalu parameter.	8.8	More Details
CVE-2024-37802	CodeProjects Health Care hospital Management System v1.0 was discovered to contain a SQL injection vulnerability in the Patient Info module via the searvalu parameter.	8.8	More Details
CVE-2024-6045	Certain models of D-Link wireless routers contain an undisclosed factory testing backdoor. Unauthenticated attackers on the local area network can force the device to enable Telnet service by accessing a specific URL and can log in by using the administrator credentials obtained from analyzing the firmware.	8.8	More Details
CVE-2024-2698	A vulnerability was found in FreeIPA in how the initial implementation of MS-SFU by MIT Kerberos was missing a condition for granting the "forwardable" flag on S4U2Self tickets. Fixing this mistake required adding a special case for the check_allowed_to_delegate() function: If the target service argument is NULL, then it means the KDC is probing for general constrained delegation rules and not checking a specific S4U2Proxy request. In FreeIPA 4.11.0, the behavior of ipadb_match_acl() was modified to match the changes from upstream MIT Kerberos 1.20. However, a mistake resulting in this mechanism applies in cases where the target service argument is set AND where it is unset. This results in S4U2Proxy requests being accepted regardless of whether or not there is a matching service delegation rule.	8.8	More Details
CVE-2024-37639	TOTOLINK A3700R V9.1.2u.6165_20211012 was discovered to contain a stack overflow via eport in the function setIpPortFilterRules.	8.8	More Details
CVE-2024-37640	TOTOLINK A3700R V9.1.2u.6165_20211012 was discovered to contain a stack overflow via ssid5g in the function setWiFiEasyGuestCfg.	8.8	More Details
CVE-2024-37630	D-Link DIR-605L v2.13B01 was discovered to contain a hardcoded password vulnerability in /etc/passwd, which allows attackers to log in as root.	8.8	More Details
CVE-2024-36586	An issue in AdGuardHome v0.93 to latest allows unprivileged attackers to escalate privileges via overwriting the AdGuardHome binary.	8.8	More Details
CVE-2024-33620	Absolute path traversal vulnerability exists in ID Link Manager and FUJITSU Software TIME CREATOR. If this vulnerability is exploited, the file contents including sensitive information on the server may be retrieved by an unauthenticated remote attacker.	8.6	More Details
CVE-2024-5650	DLL Hijacking vulnerability has been found in CENTUM CAMS Log server provided by Yokogawa Electric Corporation. If an attacker is somehow able to intrude into a computer that installed affected product or access to a shared folder, by replacing the DLL file with a tampered one, it is possible to execute arbitrary programs with the authority of the SYSTEM account. The affected products and versions are as follows: CENTUM CS 3000 R3.08.10 to R3.09.50 CENTUM VP R4.01.00 to R4.03.00, R5.01.00 to R5.04.20, R6.01.00 to R6.11.10.	8.5	More Details
CVE-2024-4404	The ElementsKit PRO plugin for WordPress is vulnerable to Server-Side Request Forgery in versions up to, and including, 3.6.2 via the 'render_raw' function. This can allow authenticated attackers, with contributor-level permissions and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31956	An issue was discovered in Samsung Mobile Processor Exynos 2200, Exynos 1480, Exynos 2400. It lacks proper buffer length checking, which can result in an Out-of-Bounds Write.	8.4	More Details
CVE-2024-32504	An issue was discovered in Samsung Mobile Processor and Wearable Processor Exynos 850, Exynos 1080, Exynos 2100, Exynos 1280, Exynos 1380, Exynos 1330, Exynos W920, Exynos W930. The mobile processor lacks proper length checking, which can result in an OOB (Out-of-Bounds) Write vulnerability.	8.4	More Details
CVE-2024-36600	Buffer Overflow Vulnerability in libcdio v2.1.0 allows an attacker to execute arbitrary code via a crafted ISO 9660 image file.	8.4	More Details
CVE-2024-37848	SQL Injection vulnerability in Online-Bookstore-Project-In-PHP v1.0 allows a local attacker to execute arbitrary code via the admin_delete.php component.	8.4	More Details
CVE-2024-27169	Toshiba printers provides API without authentication for internal access. A local attacker can bypass authentication in applications, providing administrative access. As for the affected products/models/versions, see the reference URL.	8.4	More Details
CVE-2024-36577	apphp js-object-resolver < 3.1.1 is vulnerable to Prototype Pollution via Module.setNestedProperty.	8.3	More Details
CVE-2024-34104	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized access, leading to both confidentiality and integrity impact. Exploitation of this issue does not require user interaction.	8.2	More Details
CVE-2024-37305	oqs-provider is a provider for the OpenSSL 3 cryptography library that adds support for post-quantum cryptography in TLS, X.509, and S/MIME using post-quantum algorithms from liboqs. Flaws have been identified in the way oqs-provider handles lengths decoded with DECODE_UINT32 at the start of serialized hybrid (traditional + post-quantum) keys and signatures. Unchecked length values are later used for memory reads and writes; malformed input can lead to crashes or information leakage. Handling of plain/non-hybrid PQ key operation is not affected. This issue has been patched in in v0.6.1. All users are advised to upgrade. There are no workarounds for this issue.	8.2	More Details
CVE-2022-23829	A potential weakness in AMD SPI protection features may allow a malicious attacker with Ring0 (kernel mode) access to bypass the native System Management Mode (SMM) ROM protections.	8.2	More Details
CVE-2024-36583	A Prototype Pollution issue in byondreal accessor <= 1.0.0 allows an attacker to execute arbitrary code via @byondreal/accessor/index.	8.1	More Details
CVE-2024-37882	Nextcloud Server is a self hosted personal cloud system. A recipient of a share with read&share permissions could reshare the item with more permissions. It is recommended that the Nextcloud Server is upgraded to 26.0.13 or 27.1.8 or 28.0.4 and that the Nextcloud Enterprise Server is upgraded to 26.0.13 or 27.1.8 or 28.0.4.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37300	OAuthenticator is software that allows OAuth2 identity providers to be plugged in and used with JupyterHub. JupyterHub < 5.0, when used with `GlobusOAuthenticator`, could be configured to allow all users from a particular institution only. This worked fine prior to JupyterHub 5.0, because `allow_all` did not take precedence over `identity_provider`. Since JupyterHub 5.0, `allow_all` does take precedence over `identity_provider`. On a hub with the same config, now all users will be allowed to login, regardless of `identity_provider`. `identity_provider` will basically be ignored. This is a documented change in JupyterHub 5.0, but is likely to catch many users by surprise. OAuthenticator 16.3.1 fixes the issue with JupyterHub 5.0, and does not affect previous versions. As a workaround, do not upgrade to JupyterHub 5.0 when using `GlobusOAuthenticator` in the prior configuration.	8.1	More Details
CVE-2024-32929	In gpu_slc_get_region of pixel_gpu_slc.c, there is a possible EoP due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.1	More Details
CVE-2024-5154	A flaw was found in cri-o. A malicious container can create a symbolic link to arbitrary files on the host via directory traversal ("../"). This flaw allows the container to read and write to arbitrary files on the host system.	8.1	More Details
CVE-2024-3183	A vulnerability was found in FreeIPA in a way when a Kerberos TGS-REQ is encrypted using the client's session key. This key is different for each new session, which protects it from brute force attacks. However, the ticket it contains is encrypted using the target principal key directly. For user principals, this key is a hash of a public per-principal randomly-generated salt and the user's password. If a principal is compromised it means the attacker would be able to retrieve tickets encrypted to any principal, all of them being encrypted by their own key directly. By taking these tickets and salts offline, the attacker could run brute force attacks to find character strings able to decrypt tickets when combined to a principal salt (i.e. find the principal's password).	8.1	More Details
CVE-2024-34694	LNbits is a Lightning wallet and accounts system. Paying invoices in Eclair that do not get settled within the internal timeout (about 30s) lead to a payment being considered failed, even though it may still be in flight. This vulnerability can lead to a total loss of funds for the node backend. This vulnerability is fixed in 0.12.6.	8.1	More Details
CVE-2023-6696	The Popup Builder – Create highly converting, mobile friendly marketing popups. plugin for WordPress is vulnerable to unauthorized access of functionality due to a missing capability check on several functions in all versions up to, and including, 4.3.1. While some functions contain a nonce check, the nonce can be obtained from the profile page of a logged-in user. This allows subscribers to perform several actions including deleting subscribers and perform blind Server-Side Request Forgery.	8.1	More Details
CVE-2024-33377	LB-LINK BL-W1210M v2.0 was discovered to contain a clickjacking vulnerability via the Administrator login page. Attackers can cause victim users to perform arbitrary operations via interaction with crafted elements on the web page.	8.1	More Details
CVE-2024-36598	An arbitrary file upload vulnerability in Aegon Life v1.0 allows attackers to execute arbitrary code via uploading a crafted image file.	8.1	More Details
CVE-2024-37037	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could allow an authenticated user with access to the device's web interface to corrupt files and impact device functionality when sending a crafted HTTP request.	8.1	More Details
CVE-2024-34103	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction, but attack complexity is high.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5543	The Slideshow Gallery LITE plugin for WordPress is vulnerable to time-based SQL Injection via the id parameter in all versions up to, and including, 1.8.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.1	More Details
CVE-2024-36263	** UNSUPPORTED WHEN ASSIGNED ** Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Submarine Server Core. This issue affects Apache Submarine Server Core: all versions. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an alternative or restrict access to the instance to trusted users. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	8.1	More Details
CVE-2024-36502	Out-of-bounds read vulnerability in the audio module Impact: Successful exploitation of this vulnerability will affect availability.	7.9	More Details
CVE-2024-37307	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Starting in version 1.13.0 and prior to versions 1.13.7, 1.14.12, and 1.15.6, the output of `cilium-bugtool` can contain sensitive data when the tool is run (with the `--envoy-dump` flag set) against Cilium deployments with the Envoy proxy enabled. Users of the TLS inspection, Ingress with TLS termination, Gateway API with TLS termination, and Kafka network policies with API key filtering features are affected. The sensitive data includes the CA certificate, certificate chain, and private key used by Cilium HTTP Network Policies, and when using Ingress/Gateway API and the API keys used in Kafka-related network policy. `cilium-bugtool` is a debugging tool that is typically invoked manually and does not run during the normal operation of a Cilium cluster. This issue has been patched in Cilium v1.15.6, v1.14.12, and v1.13.17. There is no workaround to this issue.	7.9	More Details
CVE-2024-27165	Toshiba printers contain a suidperl binary and it has a Local Privilege Escalation vulnerability. A local attacker can get root privileges. As for the affected products/models/versions, see the reference URL.	7.8	More Details
CVE-2024-32896	there is a possible way to bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2024-0865	CWE-798: Use of hard-coded credentials vulnerability exists that could cause local privilege escalation when logged in as a non-administrative user.	7.8	More Details
CVE-2024-20753	Photoshop Desktop versions 24.7.3, 25.7 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-34115	Substance3D - Stager versions 2.1.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-37022	Fuji Electric Tellus Lite V-Simulator is vulnerable to an out-of-bounds write, which could allow an attacker to manipulate memory, resulting in execution of arbitrary code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37029	Fuji Electric Tellus Lite V-Simulator is vulnerable to a stack-based buffer overflow, which could allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2024-2747	CWE-428: Unquoted search path or element vulnerability exists in Easergy Studio, which could cause privilege escalation when a valid user replaces a trusted file name on the system and reboots the machine.	7.8	More Details
CVE-2024-36587	Insecure permissions in DNSCrypt-proxy v2.0.0alpha9 to v2.1.5 allows non-privileged attackers to escalate privileges to root via overwriting the binary dnscrypt-proxy.	7.8	More Details
CVE-2024-29784	In prepare_response of lwis_periodic_io.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-32892	In handle_init of goodix/main/main.c, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-32895	In BCMFASTPATH of dhd_msgbuf.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-3498	Attackers can then execute malicious files by enabling certain services of the printer via the web configuration page and elevate its privileges to root. As for the affected products/models/versions, see the reference URL.	7.8	More Details
CVE-2024-32900	In lwis_fence_signal of lwis_debug.c, there is a possible Use after Free due to improper locking. This could lead to local escalation of privilege from hal_camera_default SELinux label with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-0099	NVIDIA vGPU software for Linux contains a vulnerability in the Virtual GPU Manager, where the guest OS could cause buffer overrun in the host. A successful exploit of this vulnerability might lead to information disclosure, data tampering, escalation of privileges, and denial of service.	7.8	More Details
CVE-2024-32901	In v4l2_smfc_qbuf of smfc-v4l2-ioctls.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-32903	In prepare_response_locked of lwis_transaction.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-32906	In AcvpOnMessage of avcp.cpp, there is a possible EOP due to uninitialized data. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-32907	In memcall_add of memlog.c, there is a possible buffer overflow due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-36500	Privilege escalation vulnerability in the AMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32909	In handle_msg of main.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-32919	In lwis_add_completion_fence of lwis_fence.c, there is a possible escalation of privilege due to type confusion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-0084	NVIDIA vGPU software for Linux contains a vulnerability in the Virtual GPU Manager, where the guest OS could execute privileged operations. A successful exploit of this vulnerability might lead to information disclosure, data tampering, escalation of privileges, and denial of service.	7.8	More Details
CVE-2024-3467	There is a vulnerability in AVEVA PI Asset Framework Client that could allow malicious code to execute on the PI System Explorer environment under the privileges of an interactive user that was socially engineered to import XML supplied by an attacker.	7.8	More Details
CVE-2024-0089	NVIDIA GPU Display Driver for Windows contains a vulnerability where the information from a previous client or another process could be disclosed. A successful exploit of this vulnerability might lead to code execution, information disclosure, or data tampering.	7.8	More Details
CVE-2024-0090	NVIDIA GPU driver for Windows and Linux contains a vulnerability where a user can cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2024-0091	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability where a user can cause an untrusted pointer dereference by executing a driver API. A successful exploit of this vulnerability might lead to denial of service, information disclosure, and data tampering.	7.8	More Details
CVE-2024-32908	In sec_media_protect of media.c, there is a possible permission bypass due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-29787	In lwis_process_transactions_in_queue of lwis_transaction.c, there is a possible use after free due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-28964	Dell Common Event Enabler, version 8.9.10.0 and prior, contain an insecure deserialization vulnerability in CAVATools. A local unauthenticated attacker could potentially exploit this vulnerability, leading to arbitrary code execution in the context of the logged in user. Exploitation of this issue requires a victim to open a malicious file.	7.8	More Details
CVE-2024-6080	A vulnerability classified as critical was found in Intelbras InControl 2.21.56. This vulnerability affects unknown code of the component incontrolWebcam Service. The manipulation leads to unquoted search path. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. Upgrading to version 2.21.58 is able to address this issue. It is recommended to upgrade the affected component. The vendor was contacted early about this disclosure and plans to provide a solution within the next few weeks.	7.8	More Details
CVE-2024-38459	langchain_experimental (aka LangChain Experimental) before 0.0.61 for LangChain provides Python REPL access without an opt-in step. NOTE; this issue exists because of an incomplete fix for CVE-2024-27444.	7.8	More Details
CVE-2024-37081	The vCenter Server contains multiple local privilege escalation vulnerabilities due to misconfiguration of sudo. An authenticated local user with non-administrative privileges may exploit these issues to elevate privileges to root on vCenter Server Appliance.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22002	CORSAIR iCUE 5.9.105 with iCUE Murals on Windows allows unprivileged users to insert DLL files in the cuepkg-1.2.6 subdirectory of the installation directory.	7.8	More Details
CVE-2024-5275	A hard-coded password in the FileCatalyst TransferAgent can be found which can be used to unlock the keystore from which contents may be read out, for example, the private key for certificates. Exploit of this vulnerability could lead to a machine-in-the-middle (MiTM) attack against users of the agent. This issue affects all versions of FileCatalyst Direct from 3.8.10 Build 138 and earlier and all versions of FileCatalyst Workflow from 5.1.6 Build 130 and earlier.	7.8	More Details
CVE-2024-38449	A Directory Traversal vulnerability in KasmVNC 1.3.1.230e50f7b89663316c70de7b0e3db6f6b9340489 and possibly earlier versions allows remote authenticated attackers to browse parent directories and read the content of files outside the scope of the application.	7.7	More Details
CVE-2024-27155	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. The programs can be replaced by malicious programs by any local or remote attacker. As for the affected products/models/versions, see the reference URL.	7.7	More Details
CVE-2024-5685	Users with "User:edit" and "Self:api" permissions can promote or demote themselves or other users by performing changes to the group's memberships via API call.This issue affects snipe-it: from v4.6.17 through v6.4.1.	7.6	More Details
CVE-2024-36581	A Prototype Pollution issue in abw badger-database 1.2.1 allows an attacker to execute arbitrary code via dist/badger-database.esm.	7.6	More Details
CVE-2024-38467	Shenzhen Guoxin Synthesis image system before 8.3.0 allows unauthorized user information retrieval via the queryUser API.	7.5	More Details
CVE-2024-4032	The “ipaddress” module contained incorrect information about whether certain IPv4 and IPv6 addresses were designated as “globally reachable” or “private”. This affected the is_private and is_global properties of the ipaddress.IPv4Address, ipaddress.IPv4Network, ipaddress.IPv6Address, and ipaddress.IPv6Network classes, where values wouldn’t be returned in accordance with the latest information from the IANA Special-Purpose Address Registries. CPython 3.12.4 and 3.13.0a6 contain updated information from these registries and thus have the intended behavior.	7.5	More Details
CVE-2024-32860	Dell Client Platform BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	7.5	More Details
CVE-2024-32902	Remote prevention of access to cellular service with no user interaction (for example, crashing the cellular radio service with a malformed packet)	7.5	More Details
CVE-2024-26029	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain disclose information. Exploitation of this issue does not require user interaction.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37131	SCG Policy Manager, all versions, contains an overly permissive Cross-Origin Resource Policy (CORP) vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the execution of malicious actions on the application in the context of the authenticated user.	7.5	More Details
CVE-2024-2098	The Download Manager plugin for WordPress is vulnerable to unauthorized access of data due to an improper authorization check on the 'protectMediaLibrary' function in all versions up to, and including, 3.2.89. This makes it possible for unauthenticated attackers to download password-protected files.	7.5	More Details
CVE-2024-5908	A problem with the Palo Alto Networks GlobalProtect app can result in exposure of encrypted user credentials, used for connecting to GlobalProtect, in application logs. Normally, these application logs are only viewable by local users and are included when generating logs for troubleshooting purposes. This means that these encrypted credentials are exposed to recipients of the application logs.	7.5	More Details
CVE-2023-48280	Missing Authorization vulnerability in Consensu.IO Consensu.Io.This issue affects Consensu.Io: from n/a through 1.0.1.	7.5	More Details
CVE-2024-38461	irodsServerMonPerf in iRODS before 4.3.2 attempts to proceed with use of a path even if it is not a directory.	7.5	More Details
CVE-2024-38440	Netatalk before 3.2.1 has an off-by-one error, and resultant heap-based buffer overflow and segmentation violation, because of incorrectly using FPLoginExt in BN_bin2bn in etc/uams/uams_dhx_pam.c. The original issue 1097 report stated: 'The latest version of Netatalk (v3.2.0) contains a security vulnerability. This vulnerability arises due to a lack of validation for the length field after parsing user-provided data, leading to an out-of-bounds heap write of one byte (\0). Under specific configurations, this can result in reading metadata of the next heap block, potentially causing a Denial of Service (DoS) under certain heap layouts or with ASAN enabled. ... The vulnerability is located in the FPLoginExt operation of Netatalk, in the BN_bin2bn function found in /etc/uams/uams_dhx_pam.c ... if (!(bn = BN_bin2bn((unsigned char *)ibuf, KEYSIZE, NULL))) ... threads ... [#0] Id 1, Name: "afpd", stopped 0x7ffff4304e58 in ?? (), reason: SIGSEGV ... [#0] 0x7ffff4304e58 mov BYTE PTR [r14+0x8], 0x0 ... mov rdx, QWORD PTR [rsp+0x18] ... afp_login_ext(obj=<optimized out>, ibuf=0x62d000010424 "", ibuflen=0xfffffffffffff0015, rbuf=<optimized out>, rbuflen=<optimized out>) ... afp_over_dsi(obj=0x5555556154c0 <obj>).' 2.4.1 and 3.1.19 are also fixed versions.	7.5	More Details
CVE-2024-32859	Dell Client Platform BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	7.5	More Details
CVE-2024-4696	A privilege escalation vulnerability was reported in Lenovo Service Bridge prior to version 5.0.2.17 that could allow operating system commands to be executed if a specially crafted link is visited.	7.5	More Details
CVE-2024-32894	In bc_get_converted_received_bearer of bc_utilities.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2024-30472	Telemetry Dashboard v1.0.0.8 for Dell ThinOS 2402 contains a sensitive information disclosure vulnerability. An unauthenticated user with local access to the device could exploit this vulnerability leading to information disclosure.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29781	In ss_AnalyzeOssReturnResUssdArgIe of ss_OssAsnManagement.c, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2024-37890	ws is an open source WebSocket client and server for Node.js. A request with a number of headers exceeding theserver.maxHeadersCount threshold could be used to crash a ws server. The vulnerability was fixed in ws@8.17.1 (e55e510) and backported to ws@7.5.10 (22c2876), ws@6.2.3 (eeb76d3), and ws@5.2.4 (4abd8f6). In vulnerable versions of ws, the issue can be mitigated in the following ways: 1. Reduce the maximum allowed length of the request headers using the --max-http-header-size=size and/or the maxHeaderSize options so that no more headers than the server.maxHeadersCount limit can be sent. 2. Set server.maxHeadersCount to 0 so that no limit is applied.	7.5	More Details
CVE-2024-36856	RMQTT Broker 0.4.0 allows remote attackers to cause a Denial of Service (daemon crash) via a certain sequence of five TCP packets.	7.5	More Details
CVE-2024-5551	The WP STAGING Pro WordPress Backup Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.6.0. This is due to missing or incorrect nonce validation on the 'sub' parameter called from the WP STAGING WordPress Backup Plugin - Backup Duplicator & Migration plugin. This makes it possible for unauthenticated attackers to include any local files that end in '-settings.php' via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	7.5	More Details
CVE-2024-37038	CWE-276: Incorrect Default Permissions vulnerability exists that could allow an authenticated user with access to the device’s web interface to perform unauthorized file and firmware uploads when crafting custom web requests.	7.5	More Details
CVE-2024-37367	A user authentication vulnerability exists in the Rockwell Automation FactoryTalk® View SE v12. The vulnerability allows a user from a remote system with FTView to send a packet to the customer’s server to view an HMI project. This action is allowed without proper authentication verification.	7.5	More Details
CVE-2024-36760	A stack overflow vulnerability was found in version 1.18.0 of rhai. The flaw position is: (/SRC/rhai/SRC/eval/STMT. Rs in rhai: : eval: : STMT: : _ $LT $impl $u20 $rhai.. engine.. Engine$GT$::eval_stmt::h3f1d68ce37fc6e96). Due to the stack overflow is a recursive call/SRC/rhai/SRC/eval/STMT. Rs file eval_stmt_block function.	7.5	More Details
CVE-2024-37795	A segmentation fault in CVC5 Solver v1.1.3 allows attackers to cause a Denial of Service (DoS) via a crafted SMT-LIB input file containing the `set-logic` command with specific formatting errors.	7.5	More Details
CVE-2024-34112	ColdFusion versions 2023u7, 2021u13 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could exploit this vulnerability to gain unauthorized access to sensitive files or data. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2024-38275	The cURL wrapper in Moodle retained the original request headers when following redirects, so HTTP authorization header information could be unintentionally sent in requests to redirect URLs.	7.5	More Details
CVE-2024-34129	Acrobat Mobile Sign Android versions 24.4.2.33155 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to access files and directories that are outside the restricted directory and also to overwrite arbitrary files. Exploitation of this issue does not requires user interaction and attack complexity is high.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32858	Dell Client Platform BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	7.5	More Details
CVE-2024-37794	Improper input validation in CVC5 Solver v1.1.3 allows attackers to cause a Denial of Service (DoS) via a crafted SMT2 input file.	7.5	More Details
CVE-2024-0397	A defect was discovered in the Python “ssl” module where there is a memory race condition with the ssl.SSLContext methods “cert_store_stats()” and “get_ca_certs()”. The race condition can be triggered if the methods are called at the same time as certificates are loaded into the SSLContext, such as during the TLS handshake with a certificate directory configured. This issue is fixed in CPython 3.10.14, 3.11.9, 3.12.3, and 3.13.0a5.	7.4	More Details
CVE-2024-32921	In lwis_initialize_transaction_fences of lwis_fence.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.4	More Details
CVE-2024-27275	IBM i 7.2, 7.3, 7.4, and 7.5 contains a local privilege escalation vulnerability caused by an insufficient authority requirement. A local user without administrator privilege can configure a physical file trigger to execute with the privileges of a user socially engineered to access the target file. The correction is to require administrator privilege to configure trigger support. IBM X-Force ID: 285203.	7.4	More Details
CVE-2024-2544	The Popup Builder plugin for WordPress is vulnerable to unauthorized modification of data and loss of data due to a missing capability check on all AJAX actions. This makes it possible for authenticated attackers, with subscriber-level access and above, to perform multiple unauthorized actions, such as deleting subscribers, and importing subscribers to conduct stored cross-site scripting attacks.	7.4	More Details
CVE-2024-32922	In gpu_pm_power_on_top_nolock of pixel_gpu_power.c, there is a possible compromise of protected memory due to a logic error in the code. This could lead to local escalation of privilege to TEE with no additional execution privileges needed. User interaction is not needed for exploitation.	7.4	More Details
CVE-2024-27150	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. As for the affected products/models/versions, see the reference URL.	7.4	More Details
CVE-2024-27152	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. As for the affected products/models/versions, see the reference URL.	7.4	More Details
CVE-2024-27166	Coredump binaries in Toshiba printers have incorrect permissions. A local attacker can steal confidential information. As for the affected products/models/versions, see the reference URL.	7.4	More Details
CVE-2024-27171	A remote attacker using the insecure upload functionality will be able to overwrite any Python file and get Remote Code Execution. As for the affected products/models/versions, see the reference URL.	7.4	More Details
CVE-2024-27158	All the Toshiba printers share the same hardcoded root password. As for the affected products/models/versions, see the reference URL.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27170	It was observed that all the Toshiba printers contain credentials used for WebDAV access in the readable file. Then, it is possible to get a full access with WebDAV to the printer. As for the affected products/models/versions, see the reference URL.	7.4	More Details
CVE-2024-27153	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. As for the affected products/models/versions, see the reference URL.	7.4	More Details
CVE-2024-27167	Toshiba printers use Sendmail to send emails to recipients. Sendmail is used with several insecure directories. A local attacker can inject a malicious Sendmail configuration file. As for the affected products/models/versions, see the reference URL.	7.4	More Details
CVE-2024-27151	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. The programs can be replaced by malicious programs by any local or remote attacker. As for the affected products/models/versions, see the reference URL.	7.4	More Details
CVE-2023-5527	The Business Directory Plugin plugin for WordPress is vulnerable to CSV Injection in versions up to, and including, 6.4.3 via the class-csv-exporter.php file. This allows authenticated attackers, with author-level permissions and above, to embed untrusted input into CSV files exported by administrators, which can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration.	7.4	More Details
CVE-2024-27149	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. As for the affected products/models/versions, see the reference URL.	7.4	More Details
CVE-2024-27148	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. As for the affected products/models/versions, see the reference URL.	7.4	More Details
CVE-2024-27147	The Toshiba printers are vulnerable to a Local Privilege Escalation vulnerability. An attacker can remotely compromise any Toshiba printer. As for the affected products/models/versions, see the reference URL.	7.4	More Details
CVE-2024-6084	A vulnerability has been found in itsourcecode Pool of Bethesda Online Reservation System up to 1.0 and classified as critical. Affected by this vulnerability is the function uploadImage of the file /admin/mod_room/controller.php?action=add. The manipulation of the argument image leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268825 was assigned to this vulnerability.	7.3	More Details
CVE-2024-36503	Memory management vulnerability in the Gralloc module Impact: Successful exploitation of this vulnerability will affect availability.	7.3	More Details
CVE-2024-37313	Nextcloud server is a self hosted personal cloud system. Under some circumstance it was possible to bypass the second factor of 2FA after successfully providing the user credentials. It is recommended that the Nextcloud Server is upgraded to 26.0.13, 27.1.8 or 28.0.4 and Nextcloud Enterprise Server is upgraded to 21.0.9.17, 22.2.10.22, 23.0.12.17, 24.0.12.13, 25.0.13.8, 26.0.13, 27.1.8 or 28.0.4.	7.3	More Details
CVE-2024-5896	A vulnerability, which was classified as critical, was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. Affected is the function save_users of the file /classes/Users.php?f=save. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-268140.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1094	The Timetics- AI-powered Appointment Booking with Visual Seat Plan and ultimate Calendar Scheduling plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the make_staff() function in all versions up to, and including, 1.0.21. This makes it possible for unauthenticated attackers to grant users staff permissions.	7.3	More Details
CVE-2024-5894	A vulnerability classified as critical was found in SourceCodester Online Eyewear Shop 1.0. This vulnerability affects unknown code of the file manage_product.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-268138 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-6110	A vulnerability was found in itsourcecode Magbanua Beach Resort Online Reservation System up to 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file controller.php. The manipulation of the argument image leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-268856.	7.3	More Details
CVE-2024-6065	A vulnerability was found in itsourcecode Bakery Online Ordering System 1.0. It has been rated as critical. This issue affects some unknown processing of the file index.php. The manipulation of the argument user_email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268793 was assigned to this vulnerability.	7.3	More Details
CVE-2024-5983	A vulnerability was found in itsourcecode Online Bookstore 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file bookPerPub.php. The manipulation of the argument pubid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268459.	7.3	More Details
CVE-2024-6003	A vulnerability was found in Guangdong Baolun Electronics IP Network Broadcasting Service Platform 2.0. It has been classified as critical. Affected is an unknown function of the file /api/v2/maps. The manipulation of the argument orderColumn leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-268692. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-5984	A vulnerability was found in itsourcecode Online Bookstore 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file book.php. The manipulation of the argument bookisbn leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-268460.	7.3	More Details
CVE-2024-6112	A vulnerability classified as critical was found in itsourcecode Pool of Bethesda Online Reservation System 1.0. This vulnerability affects unknown code of the file index.php. The manipulation of the argument log_email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-268858 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-6043	A vulnerability classified as critical has been found in SourceCodester Best House Rental Management System 1.0. This affects the function login of the file admin_class.php. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268767.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6042	A vulnerability was found in itsourcecode Real Estate Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file property-detail.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-268766 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-6114	A vulnerability classified as critical has been found in itsourcecode Monbela Tourist Inn Online Reservation System up to 1.0. Affected is an unknown function of the file controller.php. The manipulation of the argument image leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-268866 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-6115	A vulnerability classified as critical was found in itsourcecode Simple Online Hotel Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file add_room.php. The manipulation of the argument photo leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268867.	7.3	More Details
CVE-2024-6116	A vulnerability, which was classified as critical, has been found in itsourcecode Simple Online Hotel Reservation System 1.0. Affected by this issue is some unknown functionality of the file edit_room.php. The manipulation of the argument photo leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-268868.	7.3	More Details
CVE-2024-5976	A vulnerability was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. It has been classified as critical. Affected is the function log_employee of the file /classes/Master.php?f=log_employee. The manipulation of the argument employee_code leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-268422 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-6111	A vulnerability classified as critical has been found in itsourcecode Pool of Bethesda Online Reservation System 1.0. This affects an unknown part of the file login.php. The manipulation of the argument email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268857 was assigned to this vulnerability.	7.3	More Details
CVE-2024-34110	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution. A high-privilege attacker could exploit this vulnerability by uploading a malicious file to the system, which could then be executed. Exploitation of this issue does not require user interaction.	7.2	More Details
CVE-2024-34109	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction, but admin privileges are required.	7.2	More Details
CVE-2024-31162	The specific function parameter of ASUS Download Master does not properly filter user input. An unauthenticated remote attacker with administrative privileges can exploit this vulnerability to execute arbitrary system commands on the device.	7.2	More Details
CVE-2024-31161	The upload functionality of ASUS Download Master does not properly filter user input. Remote attackers with administrative privilege can exploit this vulnerability to upload any file to any location. They may even upload malicious web page files to the website directory, allowing arbitrary system commands to be executed upon browsing the webpage.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3079	Certain models of ASUS routers have buffer overflow vulnerabilities, allowing remote attackers with administrative privileges to execute arbitrary commands on the device.	7.2	More Details
CVE-2024-27176	An attacker can get Remote Code Execution by overwriting files. Overwriting files is enable by falsifying session ID variable. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	7.2	More Details
CVE-2024-4145	The Search & Replace WordPress plugin before 3.2.2 does not sanitize and escape a parameter before using it in a SQL statement, allowing admins to perform SQL injection attacks (such as within a multi-site network).	7.2	More Details
CVE-2024-27178	An attacker can get Remote Code Execution by overwriting files. Overwriting files is enable by falsifying file name variable. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	7.2	More Details
CVE-2024-27177	An attacker can get Remote Code Execution by overwriting files. Overwriting files is enable by falsifying package name variable. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	7.2	More Details
CVE-2024-31163	ASUS Download Master has a buffer overflow vulnerability. An unauthenticated remote attacker with administrative privileges can exploit this vulnerability to execute arbitrary system commands on the device.	7.2	More Details
CVE-2024-37621	StrongShop v1.0 was discovered to contain a Server-Side Template Injection (SSTI) vulnerability via the component /shippingOptionConfig/index.blade.php.	7.2	More Details
CVE-2024-6000	The FooEvents for WooCommerce plugin for WordPress is vulnerable to unauthorized arbitrary file uploads due to an improper capability setting on the 'display_ticket_themes_page' function in versions up to, and including, 1.19.20. This makes it possible for authenticated attackers with contributor-level capabilities or above, to upload arbitrary files on the affected site's server which may make remote code execution possible. This was partially patched in 1.19.20, and fully patched in 1.19.21.	7.1	More Details
CVE-2023-47726	IBM QRadar Suite Software 1.10.12.0 through 1.10.21.0 and IBM Cloud Pak for Security 1.10.12.0 through 1.10.21.0 could allow an authenticated user to execute certain arbitrary commands due to improper input validation. IBM X-Force ID: 272087.	7.1	More Details
CVE-2024-32920	In set_secure_reg of sac_handler.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure of 4 bytes of stack memory with no additional execution privileges needed. User interaction is not needed for exploitation.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34116	Creative Cloud Desktop versions 6.1.0.587 and earlier are affected by an Uncontrolled Search Path Element vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to load and execute malicious libraries, leading to arbitrary file delete. Exploitation of this issue requires user interaction.	7.1	More Details
CVE-2024-37306	Computer Vision Annotation Tool (CVAT) is an interactive video and image annotation tool for computer vision. Starting in version 2.2.0 and prior to version 2.14.3, if an attacker can trick a logged-in CVAT user into visiting a malicious URL, they can initiate a dataset export or a backup from a project, task or job that the victim user has permission to export into a cloud storage that the victim user has access to. The name of the resulting file can be chosen by the attacker. This implies that the attacker can overwrite arbitrary files in any cloud storage that the victim can access and, if the attacker has read access to the cloud storage used in the attack, they can obtain media files, annotations, settings and other information from any projects, tasks or jobs that the victim has permission to export. Version 2.14.3 contains a fix for the issue. No known workarounds are available.	7.1	More Details
CVE-2024-37164	Computer Vision Annotation Tool (CVAT) is an interactive video and image annotation tool for computer vision. CVAT allows users to supply custom endpoint URLs for cloud storages based on Amazon S3 and Azure Blob Storage. Starting in version 2.1.0 and prior to version 2.14.3, an attacker with a CVAT account can exploit this feature by specifying URLs whose host part is an intranet IP address or an internal domain name. By doing this, the attacker may be able to probe the network that the CVAT backend runs in for HTTP(S) servers. In addition, if there is a web server on this network that is sufficiently API-compatible with an Amazon S3 or Azure Blob Storage endpoint, and either allows anonymous access, or allows authentication with credentials that are known by the attacker, then the attacker may be able to create a cloud storage linked to this server. They may then be able to list files on the server; extract files from the server, if these files are of a type that CVAT supports reading from cloud storage (media data (such as images/videos/archives), importable annotations or datasets, task/project backups); and/or overwrite files on this server with exported annotations/datasets/backups. The exact capabilities of the attacker will depend on how the internal server is configured. Users should upgrade to CVAT 2.14.3 to receive a patch. In this release, the existing SSRF mitigation measures are applied to requests to cloud providers, with access to intranet IP addresses prohibited by default. Some workarounds are also available. One may use network security solutions such as virtual networks or firewalls to prohibit network access from the CVAT backend to unrelated servers on your internal network and/or require authentication for access to internal servers.	7.1	More Details
CVE-2024-34065	Strapi is an open-source content management system. By combining two vulnerabilities (an `Open Redirect` and `session token sent as URL query parameter`) in @strapi/plugin-users-permissions before version 4.24.2, is its possible of an unauthenticated attacker to bypass authentication mechanisms and retrieve the 3rd party tokens. The attack requires user interaction (one click). Unauthenticated attackers can leverage two vulnerabilities to obtain an 3rd party token and the bypass authentication of Strapi apps. Users should upgrade @strapi/plugin-users-permissions to version 4.24.2 to receive a patch.	7.1	More Details
CVE-2024-32917	In pl330_dma_from_peri_start() of fp_spi_dma.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.1	More Details
CVE-2024-27168	It appears that some hardcoded keys are used for authentication to internal API. Knowing these private keys may allow attackers to bypass authentication and reach administrative interfaces. As for the affected products/models/versions, see the reference URL.	7.1	More Details
CVE-2024-27164	Toshiba printers contain hardcoded credentials. As for the affected products/models/versions, see the reference URL.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32891	In sec_media_unprotect of media.c, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.0	More Details
CVE-2024-32899	In gpu_pm_power_off_top_nolock of pixel_gpu_power.c, there is a possible compromise of protected memory due to a race condition. This could lead to local escalation of privilege to TEE with no additional execution privileges needed. User interaction is not needed for exploitation.	7.0	More Details
CVE-2024-5907	A privilege escalation (PE) vulnerability in the Palo Alto Networks Cortex XDR agent on Windows devices enables a local user to execute programs with elevated privileges. However, execution does require the local user to successfully exploit a race condition, which makes this vulnerability difficult to exploit.	7.0	More Details
CVE-2024-27157	The sessions are stored in clear-text logs. An attacker can retrieve authentication sessions. A remote attacker can retrieve the credentials and bypass the authentication mechanism. As for the affected products/models/versions, see the reference URL.	6.8	More Details
CVE-2024-27156	The session cookies, used for authentication, are stored in clear-text logs. An attacker can retrieve authentication sessions. A remote attacker can retrieve the credentials and bypass the authentication mechanism. As for the affected products/models/versions, see the reference URL.	6.8	More Details
CVE-2024-5731	A vulnerability in the IPS Manager, Central Manager, and Local Manager communication workflow allows an attacker to control the destination of a request by manipulating the parameter, thereby leveraging sensitive information.	6.8	More Details
CVE-2024-4305	The Post Grid Gutenberg Blocks and WordPress Blog Plugin WordPress plugin before 4.1.0 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	6.8	More Details
CVE-2024-36499	Vulnerability of unauthorized screenshot capturing in the WMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.8	More Details
CVE-2024-36103	OS command injection vulnerability in WRC-X5400GS-B v1.0.10 and earlier, and WRC-X5400GSA-B v1.0.10 and earlier allows a network-adjacent attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to the product.	6.8	More Details
CVE-2024-0160	Dell Client Platform contains an incorrect authorization vulnerability. An attacker with physical access to the system could potentially exploit this vulnerability by bypassing BIOS authorization to modify settings in the BIOS.	6.8	More Details
CVE-2024-5742	A vulnerability was found in GNU Nano that allows a possible privilege escalation through an insecure temporary file. If Nano is killed while editing, a file it saves to an emergency file with the permissions of the running user provides a window of opportunity for attackers to escalate privileges through a malicious symlink.	6.7	More Details
CVE-2024-27146	The Toshiba printers do not implement privileges separation. As for the affected products/models/versions, see the reference URL.	6.7	More Details
CVE-2024-27180	An attacker with admin access can install rogue applications. As for the affected products/models/versions, see the reference URL.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0093	NVIDIA GPU software for Linux contains a vulnerability where it can expose sensitive information to an actor that is not explicitly authorized to have access to that information. A successful exploit of this vulnerability might lead to information disclosure.	6.5	More Details
CVE-2024-23445	It was identified that if a cross-cluster API key https://www.elastic.co/guide/en/elasticsearch/reference/8.14/security-api-create-cross-cluster-api-key.html#security-api-create-cross-cluster-api-key-request-body restricts search for a given index using the query or the field_security parameter, and the same cross-cluster API key also grants replication for the same index, the search restrictions are not enforced during cross cluster search operations and search results may include documents and terms that should not be returned. This issue only affects the API key based security model for remote clusters https://www.elastic.co/guide/en/elasticsearch/reference/8.14/remote-clusters.html#remote-clusters-security-models that was previously a beta feature and is released as GA with 8.14.0	6.5	More Details
CVE-2024-1295	The events-calendar-pro WordPress plugin before 6.4.0.1, The Events Calendar WordPress plugin before 6.4.0.1 does not prevent users with at least the contributor role from leaking details about events they shouldn't have access to. (e.g. password-protected events, drafts, etc.)	6.5	More Details
CVE-2023-40209	Missing Authorization vulnerability in Himalaya Saxena Highcompress Image Compressor.This issue affects Highcompress Image Compressor: from n/a through 6.0.0.	6.5	More Details
CVE-2024-33622	Missing authentication for critical function vulnerability exists in ID Link Manager and FUJITSU Software TIME CREATOR. If this vulnerability is exploited, sensitive information may be obtained and/or the information stored in the database may be altered by a remote authenticated attacker.	6.5	More Details
CVE-2024-1634	The Scheduling Plugin – Online Booking for WordPress plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'cbsb_disconnect_settings' function in all versions up to, and including, 3.5.10. This makes it possible for unauthenticated attackers to disconnect the plugin from the startbooking service and remove connection data.	6.5	More Details
CVE-2024-37889	MyFinances is a web application for managing finances. MyFinances has a way to access other customer invoices while signed in as a user. This method allows an actor to access PII and financial information from another account. The vulnerability is fixed in 0.4.6.	6.5	More Details
CVE-2024-5868	The WooCommerce - Social Login plugin for WordPress is vulnerable to Email Verification in all versions up to, and including, 2.6.2 via the use of insufficiently random activation code. This makes it possible for unauthenticated attackers to bypass the email verification.	6.5	More Details
CVE-2024-5313	CWE-668: Exposure of the Resource Wrong Sphere vulnerability exists that exposes a SSH interface over the product network interface. This does not allow to directly exploit the product or make any unintended operation as the SSH interface access is protected by an authentication mechanism. Impacts are limited to port scanning and fingerprinting activities as well as attempts to perform a potential denial of service attack on the exposed SSH interface.	6.5	More Details
CVE-2023-51495	Missing Authorization vulnerability in Woo WooCommerce Warranty Requests.This issue affects WooCommerce Warranty Requests: from n/a through 2.2.7.	6.5	More Details
CVE-2024-5056	CWE-552: Files or Directories Accessible to External Parties vulnerability exists which may prevent user to update the device firmware and prevent proper behavior of the webserver when specific files or directories are removed from the filesystem.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36527	puppeteer-renderer v.3.2.0 and before is vulnerable to Directory Traversal. Attackers can exploit the URL parameter using the file protocol to read sensitive information from the server.	6.5	More Details
CVE-2024-34111	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require user interaction..	6.5	More Details
CVE-2024-5674	The Newsletter - API v1 and v2 addon plugin for WordPress is vulnerable to unauthorized subscribers management due to PHP type juggling issue on the check_api_key function in all versions up to, and including, 2.4.5. This makes it possible for unauthenticated attackers to list, create or delete newsletter subscribers. This issue affects only sites running the PHP version below 8.0	6.5	More Details
CVE-2024-5468	The WordPress Header Builder Plugin – Pearl plugin for WordPress is vulnerable to unauthorized site option deletion due to a missing validation and capability checks on the stm_hb_delete() function in all versions up to, and including, 1.3.7. This makes it possible for unauthenticated attackers to delete arbitrary options that can be used to perform a denial of service attack on a site.	6.5	More Details
CVE-2024-6044	Certain models of D-Link wireless routers have a path traversal vulnerability. Unauthenticated attackers on the same local area network can read arbitrary system files by manipulating the URL.	6.5	More Details
CVE-2024-36588	An issue in Annonshop.app DecentralizeJustice/ anonymousLocker commit 2b2b4 allows attackers to send messages erroneously attributed to arbitrary users via a crafted HTTP request.	6.5	More Details
CVE-2024-5741	Stored XSS in inventory tree rendering in Checkmk before 2.3.0p7, 2.2.0p28, 2.1.0p45 and 2.0.0 (EOL)	6.5	More Details
CVE-2024-31881	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to a denial of service as the server may crash when using a specially crafted query on certain columnar tables by an authenticated user. IBM X-Force ID: 287613.	6.5	More Details
CVE-2024-1963	An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.4 prior to 16.10.7, starting from 16.11 prior to 16.11.4, and starting from 17.0 prior to 17.0.2. A vulnerability in GitLab's Asana integration allowed an attacker to potentially cause a regular expression denial of service by sending specially crafted requests.	6.5	More Details
CVE-2024-27163	Toshiba printers will display the password of the admin user in clear-text and additional passwords when sending 2 specific HTTP requests to the internal API. An attacker stealing the cookie of an admin or abusing a XSS vulnerability can recover this password in clear-text and compromise the printer. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	6.5	More Details
CVE-2024-36523	An access control issue in Wvp GB28181 Pro 2.0 allows users to continue to access information in the application after deleting their own or administrator accounts. This is provided that the users do not log out of their deleted accounts.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5951	Deep Sea Electronics DSE855 Factory Reset Missing Authentication Denial-of-Service Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of Deep Sea Electronics DSE855 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the web-based UI. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-23173.	6.5	More Details
CVE-2023-36504	Missing Authorization vulnerability in BBS e-Theme BBS e-Popup.This issue affects BBS e-Popup: from n/a through 2.4.5.	6.5	More Details
CVE-2024-5949	Deep Sea Electronics DSE855 Multipart Boundary Infinite Loop Denial-of-Service Vulnerability. This vulnerability allows network-adjacent attackers to create a denial-of-service condition on affected installations of Deep Sea Electronics DSE855 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of multipart boundaries. The issue results from a logic error that can lead to an infinite loop. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-23171.	6.5	More Details
CVE-2024-5952	Deep Sea Electronics DSE855 Restart Missing Authentication Denial-of-Service Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of Deep Sea Electronics DSE855 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the web-based UI. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-23174.	6.5	More Details
CVE-2024-5947	Deep Sea Electronics DSE855 Configuration Backup Missing Authentication Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of Deep Sea Electronics DSE855 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the web-based UI. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-22679.	6.5	More Details
CVE-2024-1736	An issue has been discovered in GitLab CE/EE affecting all versions prior to 16.10.7, starting from 16.11 prior to 16.11.4, and starting from 17.0 prior to 17.0.2. A vulnerability in GitLab's CI/CD pipeline editor could allow for denial of service attacks through maliciously crafted configuration files.	6.5	More Details
CVE-2024-38312	When browsing private tabs, some data related to location history or webpage thumbnails could be persisted incorrectly within the sandboxed app bundle after app termination This vulnerability affects Firefox for iOS < 127.	6.5	More Details
CVE-2024-1495	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.1 prior to 16.10.7, starting from 16.11 prior to 16.11.4, and starting from 17.0 prior to 17.0.2. It was possible for an attacker to cause a denial of service using maliciously crafted file.	6.5	More Details
CVE-2023-29174	Missing Authorization vulnerability in NervyThemes SKU Label Changer For WooCommerce.This issue affects SKU Label Changer For WooCommerce: from n/a through 3.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4615	The Elespare – Blog, Magazine and Newspaper Addons for Elementor with Templates, Widgets, Kits, and Header/Footer Builder. One Click Import: No Coding Required! plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Horizontal Nav Menu' widget in all versions up to, and including, 3.1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5265	The WPBakery Visual Composer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the link attribute within the vc_single_image shortcode in all versions up to, and including, 7.6 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-2024-1565	The EmbedPress – Embed PDF, YouTube, Google Docs, Vimeo, Wistia Videos, Audios, Maps & Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the PDF Widget URL in all versions up to, and including, 3.9.10 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-2024-3492	The Events Manager – Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'event', 'location', and 'event_category' shortcodes in all versions up to, and including, 6.4.7.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5787	The PowerPack Addons for Elementor (Free Widgets, Extensions and Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' attribute within the plugin's Link Effects widget in all versions up to, and including, 2.7.20 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-2024-5757	The Elementor Header & Footer Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the url attribute within the plugin's Site Title widget in all versions up to, and including, 1.6.35 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-2024-2695	The Shariff Wrapper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'shariff' shortcode in all versions up to, and including, 4.6.13 due to insufficient input sanitization and output escaping on user supplied attributes such as 'borderradius' and 'timestamp'. 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-2024-5611	The Stratum – Elementor Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘label_years’ attribute within the Countdown widget in all versions up to, and including, 1.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4551	The Video Gallery – YouTube Playlist, Channel Gallery by YotuWP plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.3.13 via the display function. This makes it possible for authenticated attackers, with contributor access and higher, to include and execute arbitrary php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	6.4	More Details
CVE-2024-4095	The Collapse-O-Matic plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'expand' and 'expandsub' shortcode in all versions up to, and including, 1.8.5.7 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-2024-1399	The Restaurant Menu – Food Ordering System – Table Reservation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 2.4.0 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-2024-5263	The ElementsKit Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Motion Text and Table widgets in all versions up to, and including, 3.6.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4479	The Jeg Elementor Kit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the sg_general_toggle_tab_enable and sg_accordion_style attributes within the plugin's JKit - Tabs and JKit - Accordion widget, respectively, in all versions up to, and including, 2.6.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with 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-2024-5558	CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability exists that could cause escalation of privileges when an attacker abuses a limited admin account.	6.4	More Details
CVE-2024-5994	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Custom JS option in versions up to, and including, 9.0.38. This makes it possible for authenticated attackers that have been explicitly granted permissions by an administrator, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Version 9.0.39 adds a caution to make administrators aware of the possibility for abuse if permissions are granted to lower-level users.	6.4	More Details
CVE-2024-2122	The Best WordPress Gallery Plugin – FooGallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via album gallery custom URLs in all versions up to, and including, 2.4.15 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-2024-4863	The Gutenberg Blocks with AI by Kadence WP – Page Builder Features plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'titleFont' parameter in all versions up to, and including, 3.2.38 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-2024-5970	The MaxGalleria plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's maxgallery_thumb shortcode in all versions up to, and including, 6.4.4 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-2024-5533	The Divi theme for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 4.25.1 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 an injected page.	6.4	More Details
CVE-2024-4892	The BuddyPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'display_name' parameter in versions up to, and including, 12.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4375	The Master Slider – Responsive Touch Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ms_layer' shortcode in all versions up to, and including, 3.9.10 due to insufficient input sanitization and output escaping on the 'css_id' user supplied attribute. 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-2024-5892	The Divi Torque Lite – Divi Theme and Extra Theme plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'support_unfiltered_files_upload' function in all versions up to, and including, 3.6.6 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 an injected page.	6.4	More Details
CVE-2024-4564	The CoDesigner WooCommerce Builder for Elementor – Customize Checkout, Shop, Email, Products & More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Shop Slider, Tabs Classic, and Image Comparison widgets in all versions up to, and including, 4.4.1 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-2024-3559	The Custom Field Suite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the the 'cfs[post_content]' parameter versions up to, and including, 2.6.7 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-2024-5266	The Download Manager Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via wpdm_user_dashboard, wpdm_package, wpdm_packages, wpdm_search_result, and wpdm_tag shortcodes in all versions up to, and including, 3.2.92 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-2024-0845	The PDF Viewer for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the render function in all versions up to, and including, 2.9.3 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-2024-3925	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Creative Button widget in all versions up to, and including, 5.6.7 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-2024-37661	TP-LINK TL-7DR5130 v1.0.23 is vulnerable to forged ICMP redirect message attacks. An attacker in the same WLAN as the victim can hijack the traffic between the victim and any remote server by sending out forged ICMP redirect messages.	6.3	More Details
CVE-2024-6008	A vulnerability, which was classified as critical, was found in itsourcecode Online Book Store up to 1.0. Affected is an unknown function of the file /edit_book.php. The manipulation of the argument image leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-268698 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-6007	A vulnerability classified as critical has been found in Netentsec NS-ASG Application Security Gateway 6.3. This affects an unknown part of the file /protocol/iscgwtunnel/deleteiscgwrouteconf.php. The manipulation of the argument messagecontent leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268695. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-37662	TP-LINK TL-7DR5130 v1.0.23 is vulnerable to TCP DoS or hijacking attacks. An attacker in the same WLAN as the victim can disconnect or hijack the traffic between the victim and any remote server by sending out forged TCP RST messages to evict NAT mappings in the router.	6.3	More Details
CVE-2024-6109	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file addmeasurement.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268855.	6.3	More Details
CVE-2024-38506	In JetBrains YouTrack before 2024.2.34646 user without appropriate permissions could enable the auto-attach option for workflows	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6067	A vulnerability classified as critical was found in SourceCodester Music Class Enrollment System 1.0. Affected by this vulnerability is an unknown functionality of the file /mces/?p=class/view_class. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268795.	6.3	More Details
CVE-2024-6066	A vulnerability classified as critical has been found in SourceCodester Best House Rental Management System 1.0. Affected is an unknown function of the file payment_report.php. The manipulation of the argument month_of leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-268794 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-6013	A vulnerability was found in itsourcecode Online Book Store 1.0. It has been rated as critical. This issue affects some unknown processing of the file admin_delete.php. The manipulation of the argument bookisbn leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268721 was assigned to this vulnerability.	6.3	More Details
CVE-2024-6083	A vulnerability, which was classified as critical, was found in PHPVibe 11.0.46. Affected is an unknown function of the file /app/uploading/upload-mp3.php of the component Media Upload Page. The manipulation of the argument file leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-268824. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-5898	A vulnerability was found in itsourcecode Payroll Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file print_payroll.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-268142 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-34024	Observable response discrepancy issue exists in ID Link Manager and FUJITSU Software TIME CREATOR. If this vulnerability is exploited, an unauthenticated remote attacker may determine if a username is valid or not.	6.3	More Details
CVE-2024-36691	Insecure permissions in the AdminController.AjaxSave() method of PPGo_Jobs v2.8.0 allows authenticated attackers to arbitrarily modify users' account information.	6.3	More Details
CVE-2024-5893	A vulnerability classified as critical has been found in SourceCodester Cab Management System 1.0. This affects an unknown part of the file /cms/classes/Users.php?f=delete_client. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268137 was assigned to this vulnerability.	6.3	More Details
CVE-2024-5895	A vulnerability, which was classified as critical, has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. This issue affects the function delete_users of the file /classes/Users.php?f=delete. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268139.	6.3	More Details
CVE-2024-33373	An issue in the LB-LINK BL-W1210M v2.0 router allows attackers to bypass password complexity requirements and set single digit passwords for authentication. This vulnerability can allow attackers to access the router via a brute-force attack.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6009	A vulnerability has been found in itsourcecode Event Calendar 1.0 and classified as critical. Affected by this vulnerability is the function regConfirm/regDelete of the file process.php. The manipulation of the argument userId leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268699.	6.3	More Details
CVE-2024-37312	user_oidc app is an OpenID Connect user backend for Nextcloud. Missing access control on the ID4me endpoint allows an attacker to register an account eventually getting access to data that is available to all registered users. It is recommended that the OpenID Connect user backend is upgraded to 3.0.0 (Nextcloud 20-23), 4.0.0 (Nexcloud 24) or 5.0.0 (Nextcloud 25-28).	6.3	More Details
CVE-2024-6014	A vulnerability classified as critical has been found in itsourcecode Document Management System 1.0. Affected is an unknown function of the file edithis.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-268722 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-5985	A vulnerability classified as critical has been found in SourceCodester Best Online News Portal 1.0. This affects an unknown part of the file /admin/index.php. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268461 was assigned to this vulnerability.	6.3	More Details
CVE-2024-6041	A vulnerability was found in itsourcecode Gym Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268765 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0085	NVIDIA vGPU software for Windows and Linux contains a vulnerability where unprivileged users could execute privileged operations on the host. A successful exploit of this vulnerability might lead to data tampering, escalation of privileges, and denial of service.	6.3	More Details
CVE-2024-6016	A vulnerability, which was classified as critical, has been found in itsourcecode Online Laundry Management System 1.0. Affected by this issue is some unknown functionality of the file admin_class.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-268724.	6.3	More Details
CVE-2023-36694	Missing Authorization vulnerability in Bryan Lee Kingkong Board.This issue affects Kingkong Board: from n/a through 2.1.0.2.	6.3	More Details
CVE-2024-36574	A Prototype Pollution issue in flatten-json 1.0.1 allows an attacker to execute arbitrary code via module.exports.unflattenJSON (flatten-json/index.js:42)	6.3	More Details
CVE-2024-0427	The ARForms - Premium WordPress Form Builder Plugin WordPress plugin before 6.4.1 does not properly escape user-controlled input when it is reflected in some of its AJAX actions.	6.3	More Details
CVE-2024-5981	A vulnerability was found in itsourcecode Online House Rental System 1.0. It has been classified as critical. Affected is an unknown function of the file manage_user.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-268458 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6039	A vulnerability, which was classified as critical, was found in Feng Office 3.11.1.2. Affected is an unknown function of the component Workspaces. The manipulation of the argument dim leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-268752.	6.3	More Details
CVE-2024-6015	A vulnerability classified as critical was found in itsourcecode Online House Rental System 1.0. Affected by this vulnerability is an unknown functionality of the file manage_user.php. The manipulation of the argument month_of leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268723.	6.3	More Details
CVE-2024-38469	zhimengzhe iBarn v1.5 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the $search parameter at /pay.php.	6.3	More Details
CVE-2024-2300	HP Advance Mobile Applications for iOS and Android are potentially vulnerable to information disclosure when using an outdated version of the application via mobile devices.	6.2	More Details
CVE-2024-27159	All the Toshiba printers contain a shell script using the same hardcoded key to encrypt logs. An attacker can decrypt the encrypted files using the hardcoded key. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	6.2	More Details
CVE-2024-27161	all the Toshiba printers have programs containing a hardcoded key used to encrypt files. An attacker can decrypt the encrypted files using the hardcoded key. Insecure algorithm is used for the encryption. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	6.2	More Details
CVE-2024-38443	C/sorting/binary_insertion_sort.c in The Algorithms - C through e5dad3f has a segmentation fault for deep recursion, which may affect common use cases such as sorting an array of 50 elements.	6.2	More Details
CVE-2024-27160	All the Toshiba printers contain a shell script using the same hardcoded key to encrypt logs. An attacker can decrypt the encrypted files using the hardcoded key. This vulnerability can be executed in combination with other vulnerabilities and difficult to execute alone. So, the CVSS score for this vulnerability alone is lower than the score listed in the "Base Score" of this vulnerability. For detail on related other vulnerabilities, please ask to the below contact point. https://www.toshibatec.com/contacts/products/ As for the affected products/models/versions, see the reference URL.	6.2	More Details
CVE-2024-27154	Passwords are stored in clear-text logs. An attacker can retrieve passwords. As for the affected products/models/versions, see the reference URL.	6.2	More Details
CVE-2024-32918	Permission Bypass allowing attackers to disable HDCP 2.2 encryption by not completing the HDCP Key Exchange initialization steps	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37878	Cross Site Scripting vulnerability in TWCMS v.2.0.3 allows a remote attacker to execute arbitrary code via the /TWCMS-gh-pages/twcms/runtime/twcms_view/default,index.htm.php" PHP directly echoes parameters input from external sources	6.1	More Details
CVE-2023-35859	A Reflected Cross-Site Scripting (XSS) vulnerability in the blog function of Modern Campus - Omni CMS 2023.1 allows a remote attacker to inject arbitrary scripts or HTML via multiple parameters.	6.1	More Details
CVE-2024-23442	An open redirect issue was discovered in Kibana that could lead to a user being redirected to an arbitrary website if they use a maliciously crafted Kibana URL.	6.1	More Details
CVE-2024-5155	The Inquiry cart WordPress plugin through 3.4.2 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	6.1	More Details
CVE-2024-38274	Insufficient escaping of calendar event titles resulted in a stored XSS risk in the event deletion prompt.	6.1	More Details
CVE-2024-37629	SummerNote 0.8.18 is vulnerable to Cross Site Scripting (XSS) via the Code View Function.	6.1	More Details
CVE-2024-5559	CWE-327: Use of a Broken or Risky Cryptographic Algorithm vulnerability exists that could cause denial of service, device reboot, or an attacker gaining full control of the relay when a specially crafted reset token is entered into the front panel of the device.	6.1	More Details
CVE-2024-3966	The Pray For Me WordPress plugin through 1.0.4 does not sanitise and escape some parameters, which could unauthenticated visitors to perform Cross-Site Scripting attacks that trigger when an admin visits the Prayer Requests in the WP Admin	6.1	More Details
CVE-2024-27162	Toshiba printers provide a web interface that will load the JavaScript file. The file contains insecure codes vulnerable to XSS and is loaded inside all the webpages provided by the printer. An attacker can steal the cookie of an admin user. As for the affected products/models/versions, see the reference URL.	6.1	More Details
CVE-2024-5739	The in-app browser of LINE client for iOS versions below 14.9.0 contains a Universal XSS (UXSS) vulnerability. This vulnerability allows for cross-site scripting (XSS) where arbitrary JavaScript can be executed in the top frame from an embedded iframe on any displayed web site within the in-app browser. The in-app browser is usually opened by tapping on URLs contained in chat messages, and for the attack to be successful, the victim must trigger a click event on a malicious iframe. If an iframe embedded in any website can be controlled by an attacker, this vulnerability could be exploited to capture or alter content displayed in the top frame, as well as user session information. This vulnerability affects LINE client for iOS versions below 14.9.0 and does not affect other LINE clients such as LINE client for Android. Please update LINE client for iOS to version 14.9.0 or higher.	6.1	More Details
CVE-2024-37800	CodeProjects Restaurant Reservation System v1.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the Date parameter at index.php.	6.1	More Details
CVE-2024-4924	The Social Sharing Plugin WordPress plugin before 3.3.63 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36656	In MintHCM 4.0.3, a registered user can execute arbitrary JavaScript code and achieve a reflected Cross-site Scripting (XSS) attack.	6.1	More Details
CVE-2024-3032	Themify Builder WordPress plugin before 7.5.8 does not validate a parameter before redirecting the user to its value, leading to an Open Redirect issue	6.1	More Details
CVE-2024-37622	Xinhu RockOA v2.6.3 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the num parameter at /flow/flow.php.	6.1	More Details
CVE-2024-37888	The Open Link is a CKEditor plugin, extending context menu with a possibility to open link in a new tab. The vulnerability allowed to execute JavaScript code by abusing link href attribute. It affects all users using the Open Link plugin at version < **1.0.5**.	6.1	More Details
CVE-2024-37623	Xinhu RockOA v2.6.3 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the /kaoqin/tpl_kaoqin_locationchange.html component.	6.1	More Details
CVE-2024-36599	A cross-site scripting (XSS) vulnerability in Aegon Life v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the name parameter at insertClient.php.	6.1	More Details
CVE-2024-37624	Xinhu RockOA v2.6.3 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the /chajian/inputChajian.php. component.	6.1	More Details
CVE-2024-37619	StrongShop v1.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the spec_group_id parameter at /spec/index.blade.php.	6.1	More Details
CVE-2024-0979	The Dashboard Widgets Suite plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 3.4.3 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.	6.1	More Details
CVE-2024-38470	zhimengzhe iBarn v1.5 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the $search parameter at /own.php.	6.1	More Details
CVE-2024-36397	Vantiva - MediaAccess DGA2232 v19.4 - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2024-36395	Verint - CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38454	ExpressionEngine before 7.4.11 allows XSS.	6.1	More Details
CVE-2024-37625	zhimengzhe iBarn v1.5 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the $search parameter at /index.php.	6.1	More Details
CVE-2024-37304	NuGet Gallery is a package repository that powers nuget.org. The NuGetGallery has a security vulnerability related to its handling of autolinks in Markdown content. While the platform properly filters out JavaScript from standard links, it does not adequately sanitize autolinks. This oversight allows attackers to exploit autolinks as a vector for Cross-Site Scripting (XSS) attacks. When a user inputs a Markdown autolink such as `<javascript:alert(1)>`, the link is rendered without proper sanitization. This means that the JavaScript code within the autolink can be executed by the browser, leading to an XSS attack. Version 2024.05.28 contains a patch for this issue.	6.1	More Details
CVE-2024-37620	PHPVOD v4.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the id parameter at /view/admin/view.php.	6.1	More Details
CVE-2024-5661	An issue has been identified in both XenServer 8 and Citrix Hypervisor 8.2 CU1 LTSR which may allow a malicious administrator of a guest VM to cause the host to become slow and/or unresponsive.	6.0	More Details
CVE-2024-37791	DuxCMS3 v3.1.3 was discovered to contain a SQL injection vulnerability via the keyword parameter at /article/Content/index?class_id.	6.0	More Details
CVE-2024-36578	akbr update 1.0.0 is vulnerable to Prototype Pollution via update/index.js.	5.9	More Details
CVE-2024-32897	In ProtocolCdmaCallWaitingIndAdapter::GetCwInfo() of protocolsmsadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with baseband firmware compromise required. User interaction is not needed for exploitation.	5.9	More Details
CVE-2024-32916	In fvp_freq_histogram_init of fvp.c, there is a possible Information Disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.9	More Details
CVE-2024-27141	Toshiba printers use XML communication for the API endpoint provided by the printer. For the endpoint, XML parsing library is used and it is vulnerable to a time-based blind XML External Entity (XXE) vulnerability. An attacker can DoS the printers by sending a HTTP request without authentication. An attacker can exploit the XXE to retrieve information. As for the affected products/models/versions, see the reference URL.	5.9	More Details
CVE-2024-37039	CWE-252: Unchecked Return Value vulnerability exists that could cause denial of service of the device when an attacker sends a specially crafted HTTP request.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37893	Firefly III is a free and open source personal finance manager. In affected versions an MFA bypass in the Firefly III OAuth flow may allow malicious users to bypass the MFA-check. This allows malicious users to use password spraying to gain access to Firefly III data using passwords stolen from other sources. As OAuth applications are easily enumerable using an incrementing id, an attacker could try sign an OAuth application up to a users profile quite easily if they have created one. The attacker would also need to know the victims username and password. This problem has been patched in Firefly III v6.1.17 and up. Users are advised to upgrade. Users unable to upgrade should Use a unique password for their Firefly III instance and store their password securely, i.e. in a password manager.	5.9	More Details
CVE-2024-27142	Toshiba printers use XML communication for the API endpoint provided by the printer. For the endpoint, XML parsing library is used and it is vulnerable to a time-based blind XML External Entity (XXE) vulnerability. An attacker can DoS the printers. An attacker can exploit the XXE to retrieve information. As for the affected products/models/versions, see the reference URL.	5.9	More Details
CVE-2024-5465	Function vulnerabilities in the Calendar module Impact: Successful exploitation of this vulnerability will affect availability.	5.9	More Details
CVE-2024-37798	Cross-site scripting (XSS) vulnerability in search-appointment.php in the Admin Panel in Phpgurukul Beauty Parlour Management System 1.0 allows remote attackers to inject arbitrary web script or HTML via the search input field.	5.9	More Details
CVE-2024-37895	Lobe Chat is an open-source LLMs/AI chat framework. In affected versions if an attacker can successfully authenticate through SSO/Access Code, they can obtain the real backend API Key by modifying the base URL to their own attack URL on the frontend and setting up a server-side request. This issue has been addressed in version 0.162.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.7	More Details
CVE-2024-37904	Minder is an open source Software Supply Chain Security Platform. Minder's Git provider is vulnerable to a denial of service from a maliciously configured GitHub repository. The Git provider clones users repositories using the `github.com/go-git/go-git/v5` library on lines `L55-L89`. The Git provider does the following on the lines `L56-L62`. First, it sets the `CloneOptions`, specifying the url, the depth etc. It then validates the options. It then sets up an in-memory filesystem, to which it clones and Finally, it clones the repository. The `(g *Git) Clone()` method is vulnerable to a DoS attack: A Minder user can instruct Minder to clone a large repository which will exhaust memory and crash the Minder server. The root cause of this vulnerability is a combination of the following conditions: 1. Users can control the Git URL which Minder clones, 2. Minder does not enforce a size limit to the repository, 3. Minder clones the entire repository into memory. This issue has been addressed in commit `7979b43` which has been included in release version v0.0.52. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.7	More Details
CVE-2024-5953	A denial of service vulnerability was found in the 389-ds-base LDAP server. This issue may allow an authenticated user to cause a server denial of service while attempting to log in with a user with a malformed hash in their password.	5.7	More Details
CVE-2024-36501	Memory management vulnerability in the boottime module Impact: Successful exploitation of this vulnerability can affect integrity.	5.6	More Details
CVE-2024-29780	In hwbcc_ns_deprivilege of trusty/user/base/lib/hwbcc/client/hwbcc.c, there is a possible uninitialized stack data disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29785	In aur_get_state of aurora.c, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-30278	Media Encoder versions 23.6.5, 24.3 and earlier Answer: are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-30276	Audition versions 24.2, 23.6.4 and earlier Answer: are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-32893	In _s5e9865_mif_set_rate of exynos_dvfs.c, there is a possible out of bounds read due to improper casting. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-30285	Audition versions 24.2, 23.6.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service condition. An attacker could exploit this vulnerability to crash the application, leading to a denial of service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-32914	In tpu_get_int_state of tpu.c, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-32912	there is a possible persistent Denial of Service due to test/debugging code left in a production build. This could lead to local denial of service of impaired use of the device with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-32910	In handle_msg_shm_map_req of trusty/user/base/lib/spi/srv/tipc/tipc.c, there is a possible stack data disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-36976	In the Linux kernel, the following vulnerability has been resolved: Revert "media: v4l2-ctrls: show all owned controls in log_status" This reverts commit 9801b5b28c6929139d6fceeee8d739cc67bb2739. This patch introduced a potential deadlock scenario: [Wed May 8 10:02:06 2024] Possible unsafe locking scenario: [Wed May 8 10:02:06 2024] CPU0 CPU1 [Wed May 8 10:02:06 2024] ---- ---- [Wed May 8 10:02:06 2024] lock(vivid_ctrls:1620:(hdl_vid_cap)->_lock); [Wed May 8 10:02:06 2024] lock(vivid_ctrls:1608:(hdl_user_vid)->_lock); [Wed May 8 10:02:06 2024] lock(vivid_ctrls:1620:(hdl_vid_cap)->_lock); [Wed May 8 10:02:06 2024] lock(vivid_ctrls:1608:(hdl_user_vid)->_lock); For now just revert.	5.5	More Details
CVE-2024-0094	NVIDIA vGPU software for Linux contains a vulnerability in the Virtual GPU Manager, where an untrusted guest VM can cause improper control of the interaction frequency in the host. A successful exploit of this vulnerability might lead to denial of service.	5.5	More Details
CVE-2024-0086	NVIDIA vGPU software for Linux contains a vulnerability where the software can dereference a NULL pointer. A successful exploit of this vulnerability might lead to denial of service and undefined behavior in the vGPU plugin.	5.5	More Details
CVE-2024-37877	UERANSIM before 3.2.6 allows out-of-bounds read when a RLS packet is sent to gNodeB with malformed PDU length. This occurs in function readOctetString in src/utils/octet_view.cpp and in function DecodeRlsMessage in src/lib/rls/rls_pdu.cpp	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25142	Use of Web Browser Cache Containing Sensitive Information vulnerability in Apache Airflow. Airflow did not return "Cache-Control" header for dynamic content, which in case of some browsers could result in potentially storing sensitive data in local cache of the browser. This issue affects Apache Airflow: before 2.9.2. Users are recommended to upgrade to version 2.9.2, which fixes the issue.	5.5	More Details
CVE-2024-34113	ColdFusion versions 2023u7, 2021u13 and earlier are affected by a Weak Cryptography for Passwords vulnerability that could result in a security feature bypass. This vulnerability arises due to the use of insufficiently strong cryptographic algorithms or flawed implementation that compromises the confidentiality of password data. An attacker could exploit this weakness to decrypt or guess passwords, potentially gaining unauthorized access to protected resources. Exploitation of this issue does not require user interaction.	5.5	More Details
CVE-2024-32926	there is a possible information disclosure due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-0092	NVIDIA GPU Driver for Windows and Linux contains a vulnerability where an improper check or improper handling of exception conditions might lead to denial of service.	5.5	More Details
CVE-2024-5909	A problem with a protection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices allows a low privileged local Windows user to disable the agent. This issue may be leveraged by malware to disable the Cortex XDR agent and then to perform malicious activity.	5.5	More Details
CVE-2024-34130	Acrobat Mobile Sign Android versions 24.4.2.33155 and earlier are affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. An attacker could exploit this vulnerability to access confidential information. Exploitation of this issue does not require user interaction.	5.5	More Details
CVE-2024-32930	In plugin_ipc_handler of slc_plugin.c, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure of 4 bytes of stack memory with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-3815	The Newspaper theme for WordPress is vulnerable to Stored Cross-Site Scripting via attachment meta in the archive page in all versions up to, and including, 12.6.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2024-3814	The tagDiv Composer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'single' module in all versions up to, and including, 4.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2024-24051	Improper input validation of printing files in Monoprice Select Mini V2 V37.115.32 allows attackers to instruct the device's movable parts to destinations that exceed the devices' maximum coordinates via the printing of a malicious .gcode file.	5.5	More Details
CVE-2024-26058	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3236	The Popup Builder WordPress plugin before 1.1.33 does not sanitise and escape some of its Notification fields, which could allow users such as contributor and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2024-26060	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-0103	NVIDIA Triton Inference Server for Linux contains a vulnerability where a user may cause an incorrect Initialization of resource by network issue. A successful exploit of this vulnerability may lead to information disclosure.	5.4	More Details
CVE-2023-51516	Missing Authorization vulnerability in Business Directory Team Business Directory Plugin.This issue affects Business Directory Plugin: from n/a through 6.3.9.	5.4	More Details
CVE-2024-33253	Cross-site scripting (XSS) vulnerability in GUnet OpenEclass E-learning Platform version 3.15 and before allows a authenticated privileged attacker to execute arbitrary code via the title and description fields of the badge template editing function.	5.4	More Details
CVE-2024-26057	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the malicious script.	5.4	More Details
CVE-2024-38277	A unique key should be generated for a user's QR login key and their auto-login key, so the same key cannot be used interchangeably between the two.	5.4	More Details
CVE-2024-26054	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2023-36695	Missing Authorization vulnerability in Maxime Schoeni Sublanguage.This issue affects Sublanguage: from n/a through 2.9.	5.4	More Details
CVE-2023-40672	Missing Authorization vulnerability in Hardik Chavada Sticky Social Media Icons.This issue affects Sticky Social Media Icons: from n/a through 2.1.	5.4	More Details
CVE-2024-26055	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script.	5.4	More Details
CVE-2024-22855	A cross-site scripting (XSS) vulnerability in the User Maintenance section of ITSS iMLog v1.307 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Last Name parameter.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26053	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	5.4	More Details
CVE-2023-51679	Missing Authorization vulnerability in BulkGate BulkGate SMS Plugin for WooCommerce.This issue affects BulkGate SMS Plugin for WooCommerce: from n/a through 3.0.2.	5.4	More Details
CVE-2024-37040	CWE-120: Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’) vulnerability exists that could allow a user with access to the device’s web interface to cause a fault on the device when sending a malformed HTTP request.	5.4	More Details
CVE-2024-37297	WooCommerce is an open-source e-commerce platform built on WordPress. A vulnerability introduced in WooCommerce 8.8 allows for cross-site scripting. A bad actor can manipulate a link to include malicious HTML & JavaScript content. While the content is not saved to the database, the links may be sent to victims for malicious purposes. The injected JavaScript could hijack content & data stored in the browser, including the session. The URL content is read through the `Sourcebuster.js` library and then inserted without proper sanitization to the classic checkout and registration forms. Versions 8.8.5 and 8.9.3 contain a patch for the issue. As a workaround, one may disable the Order Attribution feature.	5.4	More Details
CVE-2024-37886	user_oidc app is an OpenID Connect user backend for Nextcloud. An attacker could potentially trick the app into accepting a request that is not signed by the correct server. It is recommended that the Nextcloud user_oidc app is upgraded to 1.3.5, 2.0.0, 3.0.0, 4.0.0 or 5.0.0.	5.4	More Details
CVE-2023-38395	Missing Authorization vulnerability in Afzal Multani WP Clone Menu.This issue affects WP Clone Menu: from n/a through 1.0.1.	5.4	More Details
CVE-2024-4270	The SVGMagic WordPress plugin through 1.1 does not sanitize SVG file contents, which enables users with at least the author role to SVG with malicious JavaScript to conduct Stored XSS attacks.	5.4	More Details
CVE-2024-3978	The WordPress Jitsi Shortcode WordPress plugin through 0.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2024-3965	The Pray For Me WordPress plugin through 1.0.4 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	5.4	More Details
CVE-2023-51497	Missing Authorization vulnerability in Woo WooCommerce Ship to Multiple Addresses.This issue affects WooCommerce Ship to Multiple Addresses: from n/a through 3.8.9.	5.4	More Details
CVE-2023-51671	Missing Authorization vulnerability in FunnelKit FunnelKit Checkout.This issue affects FunnelKit Checkout: from n/a through 3.10.3.	5.4	More Details
CVE-2024-36169	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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 Number	Description	Base Score	Reference
CVE-2024-37799	CodeProjects Restaurant Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the reserv_id parameter at view_reservations.php.	5.4	More Details
CVE-2023-52177	Missing Authorization vulnerability in SoftLab Integrate Google Drive.This issue affects Integrate Google Drive: from n/a through 1.3.3.	5.4	More Details
CVE-2024-26039	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	5.4	More Details
CVE-2024-37803	Multiple stored cross-site scripting (XSS) vulnerabilities in CodeProjects Health Care hospital Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the fname and lname parameters under the Staff Info page.	5.4	More Details
CVE-2024-2762	The FooGallery WordPress plugin before 2.4.15, foogallery-premium WordPress plugin before 2.4.15 does not validate and escape some of its Gallery settings before outputting them back in the page, which could allow users with a role as low as Author to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admin	5.4	More Details
CVE-2024-38351	Pocketbase is an open source web backend written in go. In affected versions a malicious user may be able to compromise other user accounts. In order to be exploited users must have both OAuth2 and Password auth methods enabled. A possible attack scenario could be: 1. a malicious actor register with the targeted user's email (it is unverified), 2. at some later point in time the targeted user stumble on your app and decides to sign-up with OAuth2 (_this step could be also initiated by the attacker by sending an invite email to the targeted user_), 3. on successful OAuth2 auth we search for an existing PocketBase user matching with the OAuth2 user's email and associate them, 4. because we haven't changed the password of the existing PocketBase user during the linking, the malicious actor has access to the targeted user account and will be able to login with the initially created email/password. To prevent this for happening we now reset the password for this specific case if the previously created user wasn't verified (an exception to this is if the linking is explicit/manual, aka. when you send `Authorization:TOKEN` with the OAuth2 auth call). Additionally to warn existing users we now send an email alert in case the user has logged in with password but has at least one OAuth2 account linked. The flow will be further improved with ongoing refactoring and we will start sending emails for "unrecognized device" logins (OTP and MFA is already implemented and will be available with the next v0.23.0 release in the near future). For the time being users are advised to update to version 0.22.14. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2024-5759	An improper privilege management vulnerability exists in Tenable Security Center where an authenticated, remote attacker could view unauthorized objects and launch scans without having the required privileges	5.4	More Details
CVE-2024-38273	Insufficient capability checks meant it was possible for users to gain access to BigBlueButton join URLs they did not have permission to access.	5.4	More Details
CVE-2024-2092	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Twitter Widget in all versions up to, and including, 1.13.3 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.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20769	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-20784	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2023-27636	Progress Sitefinity before 15.0.0 allows XSS by authenticated users via the content form in the SF Editor.	5.4	More Details
CVE-2024-26036	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26037	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form.	5.4	More Details
CVE-2024-4094	The Simple Share Buttons Adder WordPress plugin before 8.5.1 does not sanitise and escape some of its settings, which could allow high privilege users such as editors to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	5.4	More Details
CVE-2024-36168	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26066	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36148	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-2024-36166	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36167	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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 Number	Description	Base Score	Reference
CVE-2024-36239	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link.	5.4	More Details
CVE-2024-36238	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a malicious link or to interact with a maliciously crafted web page.	5.4	More Details
CVE-2024-36236	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link.	5.4	More Details
CVE-2024-36235	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script.	5.4	More Details
CVE-2024-36234	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability.	5.4	More Details
CVE-2024-36233	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a malicious link.	5.4	More Details
CVE-2024-36232	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36231	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script.	5.4	More Details
CVE-2024-36230	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the execution of the malicious script.	5.4	More Details
CVE-2024-36229	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36228	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	5.4	More Details
CVE-2024-36227	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form.	5.4	More Details
CVE-2024-36225	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36224	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that causes the vulnerable script to execute.	5.4	More Details
CVE-2024-36222	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	5.4	More Details
CVE-2024-36221	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36220	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the malicious script.	5.4	More Details
CVE-2024-36219	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36218	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36165	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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 Number	Description	Base Score	Reference
CVE-2024-36164	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36163	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-28965	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for an internal enable REST API (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain Internal APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources and change of state.	5.4	More Details
CVE-2024-36150	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-29169	Dell SCG, versions prior to 5.22.00.00, contain a SQL Injection Vulnerability in the SCG UI for an internal audit REST API. A remote authenticated attacker could potentially exploit this vulnerability, leading to the execution of certain SQL commands on the application's backend database causing potential unauthorized access and modification of application data.	5.4	More Details
CVE-2024-36151	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script.	5.4	More Details
CVE-2024-36152	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36153	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-29168	Dell SCG, versions prior to 5.22.00.00, contain a SQL Injection Vulnerability in the SCG UI for an internal assets REST API. A remote authenticated attacker could potentially exploit this vulnerability, leading to the execution of certain SQL commands on the application's backend database causing potential unauthorized access and modification of application data.	5.4	More Details
CVE-2024-28968	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for internal email and collection settings REST APIs (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources and change of state.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28967	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for an internal maintenance REST API (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources and change of state.	5.4	More Details
CVE-2024-28966	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for an internal update REST API (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources and change of state.	5.4	More Details
CVE-2024-37308	The Cooked Pro recipe plugin for WordPress is vulnerable to Persistent Cross-Site Scripting (XSS) via the `_recipe_settings[post_title]` parameter in versions up to, and including, 1.7.15.4 due to insufficient input sanitization and output escaping. This vulnerability allows authenticated attackers with contributor-level access and above to inject arbitrary web scripts in pages that will execute whenever a user accesses a compromised page. A patch is available at commit 8cf88f334ccbf11134080bbb655c66f1cfe77026 and will be part of version 1.8.0.	5.4	More Details
CVE-2024-36162	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36647	A stored cross-site scripting (XSS) vulnerability in Church CRM v5.8.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Family Name parameter under the Register a New Family page.	5.4	More Details
CVE-2024-36154	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36155	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36156	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36157	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36158	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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 Number	Description	Base Score	Reference
CVE-2024-26068	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36160	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36161	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36217	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36216	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-36215	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36180	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36189	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36188	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36187	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36186	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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 Number	Description	Base Score	Reference
CVE-2024-36185	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36184	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a malicious link or to submit a specially crafted form.	5.4	More Details
CVE-2024-36183	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a malicious form.	5.4	More Details
CVE-2024-36182	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36181	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, typically in the form of convincing a victim to visit a maliciously crafted web page or to interact with a maliciously modified DOM element within the application.	5.4	More Details
CVE-2024-36179	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36191	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36178	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36177	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36176	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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 Number	Description	Base Score	Reference
CVE-2024-36175	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36174	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36173	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36172	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36171	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36170	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36190	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a user to click on a specially crafted link or to submit a form that triggers the vulnerability.	5.4	More Details
CVE-2024-36192	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36214	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36204	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36213	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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 Number	Description	Base Score	Reference
CVE-2024-36212	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36211	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-36210	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-36209	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36208	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36207	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36206	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-36205	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36203	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36193	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36202	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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 Number	Description	Base Score	Reference
CVE-2024-36201	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36200	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36199	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36198	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36197	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that triggers the vulnerability.	5.4	More Details
CVE-2024-36196	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36195	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36194	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36149	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36159	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36147	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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 Number	Description	Base Score	Reference
CVE-2024-26121	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26088	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26089	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, as the victim needs to visit a web page with a maliciously crafted script.	5.4	More Details
CVE-2024-36146	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26090	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a specially crafted link.	5.4	More Details
CVE-2024-30057	Microsoft Edge for iOS Spoofing Vulnerability	5.4	More Details
CVE-2024-36144	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-30058	Microsoft Edge (Chromium-based) Spoofing Vulnerability	5.4	More Details
CVE-2024-26091	Adobe Experience Manager versions 6.5.20 and earlier Answer: are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute.	5.4	More Details
CVE-2024-26123	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26092	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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 Number	Description	Base Score	Reference
CVE-2024-26085	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26093	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-26095	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26117	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-26116	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-26115	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-36143	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26114	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-26110	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26113	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-26086	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26111	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-36142	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-34120	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26077	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-36141	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-2024-34119	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26078	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26075	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26074	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26072	Adobe Experience Manager versions 6.5.20 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the victim's browser session. Exploitation of this issue typically requires user interaction, such as convincing a victim to click on a specially crafted link or to submit a form that causes the vulnerable script to execute.	5.4	More Details
CVE-2024-26071	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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 Number	Description	Base Score	Reference
CVE-2024-26081	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26070	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26082	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-26083	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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-2024-38465	Shenzhen Guoxin Synthesis image system before 8.3.0 allows username enumeration because of the response discrepancy of incorrect versus error.	5.3	More Details
CVE-2018-25103	There exists use-after-free vulnerabilities in lighttpd <= 1.4.50 request parsing which might read from invalid pointers to memory used in the same request, not from other requests.	5.3	More Details
CVE-2023-29267	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5is vulnerable to a denial of service, under specific configurations, as the server may crash when using a specially crafted SQL statement by an authenticated user. IBM X-Force ID: 287612.	5.3	More Details
CVE-2023-51377	Missing Authorization vulnerability in WPEverest Everest Forms.This issue affects Everest Forms: from n/a through 2.0.3.	5.3	More Details
CVE-2023-40603	Missing Authorization vulnerability in Gangesh Matta Simple Org Chart.This issue affects Simple Org Chart: from n/a through 2.3.4.	5.3	More Details
CVE-2023-51496	Missing Authorization vulnerability in Woo WooCommerce Warranty Requests.This issue affects WooCommerce Warranty Requests: from n/a through 2.2.7.	5.3	More Details
CVE-2023-41240	Missing Authorization vulnerability in Vark Pricing Deals for WooCommerce.This issue affects Pricing Deals for WooCommerce: from n/a through 2.0.3.2.	5.3	More Details
CVE-2024-23504	Missing Authorization vulnerability in WPManageNinja LLC Ninja Tables.This issue affects Ninja Tables: from n/a through 5.0.5.	5.3	More Details
CVE-2024-34106	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to gain unauthorized access or perform actions with the privileges of another user. Exploitation of this issue does not require user interaction.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34107	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and view minor unauthorised information. Exploitation of this issue does not require user interaction.	5.3	More Details
CVE-2024-36289	Reusing a nonce, key pair in encryption issue exists in "FreeFrom - the nostr client" App versions prior to 1.3.5 for Android and iOS. If this vulnerability is exploited, the content of direct messages (DMs) between users may be manipulated by a man-in-the-middle attack.	5.3	More Details
CVE-2024-36279	Reliance on obfuscation or encryption of security-relevant inputs without integrity checking issue exists in "FreeFrom - the nostr client" App versions prior to 1.3.5 for Android and iOS. If this vulnerability is exploited, the content of direct messages (DMs) between users may be manipulated by a man-in-the-middle attack.	5.3	More Details
CVE-2024-36277	Improper verification of cryptographic signature issue exists in "FreeFrom - the nostr client" App versions prior to 1.3.5 for Android and iOS. The affected app cannot detect event data with invalid signatures.	5.3	More Details
CVE-2024-4576	The component listed above contains a vulnerability that allows an attacker to traverse directories and access sensitive files, leading to unauthorized disclosure of system configuration and potentially sensitive information.	5.3	More Details
CVE-2024-31217	Strapi is an open-source content management system. Prior to version 4.22.0, a denial-of-service vulnerability is present in the media upload process causing the server to crash without restarting, affecting either development and production environments. Usually, errors in the application cause it to log the error and keep it running for other clients. This behavior, in contrast, stops the server execution, making it unavailable for any clients until it's manually restarted. Any user with access to the file upload functionality is able to exploit this vulnerability, affecting applications running in both development mode and production mode as well. Users should upgrade @strapi/plugin-upload to version 4.22.0 to receive a patch.	5.3	More Details
CVE-2023-51413	Missing Authorization vulnerability in Piotnet Forms.This issue affects Piotnet Forms: from n/a through 1.0.29.	5.3	More Details
CVE-2024-21988	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.7.0.9 and 11.8.0.5 are susceptible to disclosure of sensitive information via complex MiTM attacks due to a vulnerability in the SSH cryptographic implementation.	5.3	More Details
CVE-2024-36454	Use of uninitialized resource issue exists in IPCOM EX2 Series (V01L0x Series) V01L07NF0201 and earlier, and IPCOM VE2 Series V01L07NF0201 and earlier. If this vulnerability is exploited, the system may be rebooted or suspended by receiving a specially crafted packet.	5.3	More Details
CVE-2024-38505	In JetBrains YouTrack before 2024.2.34646 user access token was sent to the third-party site	5.3	More Details
CVE-2023-35858	XPath Injection vulnerabilities in the blog and RSS functions of Modern Campus - Omni CMS 2023.1 allow a remote, unauthenticated attacker to obtain application information.	5.3	More Details
CVE-2023-51537	Missing Authorization vulnerability in Awesome Support Team Awesome Support.This issue affects Awesome Support: from n/a through 6.1.5.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35860	A Directory Traversal vulnerability in Modern Campus - Omni CMS 2023.1 allows a remote, unauthenticated attacker to enumerate file system information via the dir parameter to listing.php or rss.php.	5.3	More Details
CVE-2024-0066	Johan Fagerström, member of the AXIS OS Bug Bounty Program, has found that a O3C feature may expose sensitive traffic between the client (Axis device) and (O3C) server. If O3C is not being used this flaw does not apply. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	5.3	More Details
CVE-2023-51507	Missing Authorization vulnerability in ExpressTech Quiz And Survey Master.This issue affects Quiz And Survey Master: from n/a through 8.1.16.	5.3	More Details
CVE-2024-5541	The Ibtana – WordPress Website Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ibtana_visual_editor_register_ajax_json_endpont' function in all versions up to, and including, 1.2.3.3. This makes it possible for unauthenticated attackers to update option values for reCAPTCHA keys on the WordPress site. This can be leveraged to bypass reCAPTCHA on the site.	5.3	More Details
CVE-2023-37394	Missing Authorization vulnerability in Deepak anand WP Dummy Content Generator.This issue affects WP Dummy Content Generator: from n/a through 2.3.0.	5.3	More Details
CVE-2024-37309	CrateDB is a distributed SQL database. A high-risk vulnerability has been identified in versions prior to 5.7.2 where the TLS endpoint (port 4200) permits client-initiated renegotiation. In this scenario, an attacker can exploit this feature to repeatedly request renegotiation of security parameters during an ongoing TLS session. This flaw could lead to excessive consumption of CPU resources, resulting in potential server overload and service disruption. The vulnerability was confirmed using an openssl client where the command `R` initiates renegotiation, followed by the server confirming with `RENEGOTIATING`. This vulnerability allows an attacker to perform a denial of service attack by exhausting server CPU resources through repeated TLS renegotiations. This impacts the availability of services running on the affected server, posing a significant risk to operational stability and security. TLS 1.3 explicitly forbids renegotiation, since it closes a window of opportunity for an attack. Version 5.7.2 of CrateDB contains the fix for the issue.	5.3	More Details
CVE-2023-35040	Missing Authorization vulnerability in SendPress SendPress Newsletters.This issue affects SendPress Newsletters: from n/a through 1.23.11.6.	5.3	More Details
CVE-2024-5560	CWE-125: Out-of-bounds Read vulnerability exists that could cause denial of service of the device’s web interface when an attacker sends a specially crafted HTTP request.	5.3	More Details
CVE-2024-6064	A vulnerability was found in GPAC 2.5-DEV-rev228-g11067ea92-master. It has been declared as problematic. This vulnerability affects the function xmt_node_end of the file src/scene_manager/loader_xmt.c of the component MP4Box. The manipulation leads to use after free. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The name of the patch is f4b3e4d2f91bc1749e7a924a8ab171af03a355a8/c1b9c794bad8f262c56f3cf690567980d96662f5. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-268792.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6128	A vulnerability, which was classified as problematic, has been found in spa-cartcms 1.9.0.6. This issue affects some unknown processing of the file /checkout of the component Checkout Page. The manipulation of the argument quantity with the input -10 leads to enforcement of behavioral workflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268895.	5.3	More Details
CVE-2024-28762	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query under certain conditions. IBM X-Force ID: 285246.	5.3	More Details
CVE-2024-37664	Redmi router RB03 v1.0.57 is vulnerable to TCP DoS or hijacking attacks. An attacker in the same WLAN as the victim can disconnect or hijack the traffic between the victim and any remote server by sending out forged TCP RST messages to evict NAT mappings in the router.	5.2	More Details
CVE-2024-32856	Dell Client Platform BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	5.1	More Details
CVE-2024-38460	In SonarQube before 10.4 and 9.9.4 LTA, encrypted values generated using the Settings Encryption feature are potentially exposed in cleartext as part of the URL parameters in the logs (such as SonarQube Access Logs, Proxy Logs, etc).	4.9	More Details
CVE-2024-37280	A flaw was discovered in Elasticsearch, affecting document ingestion when an index template contains a dynamic field mapping of “passthrough” type. Under certain circumstances, ingesting documents in this index would cause a StackOverflow exception to be thrown and ultimately lead to a Denial of Service. Note that passthrough fields is an experimental feature.	4.9	More Details
CVE-2024-31160	The parameter used in the certain page of ASUS Download Master is not properly filtered for user input. A remote attacker with administrative privilege can insert JavaScript code to the parameter for Stored Cross-site scripting attacks.	4.8	More Details
CVE-2024-5906	A cross-site scripting (XSS) vulnerability in Palo Alto Networks Prisma Cloud Compute software enables a malicious administrator with add/edit permissions for identity providers to store a JavaScript payload using the web interface on Prisma Cloud Compute. This enables a malicious administrator to perform actions in the context of another user's browser when accessed by that other user.	4.8	More Details
CVE-2024-34105	Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin 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.	4.8	More Details
CVE-2024-5172	The Expert Invoice WordPress plugin through 1.0.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-3276	The Lightbox & Modal Popup WordPress Plugin WordPress plugin before 2.7.28, foobox-image-lightbox-premium WordPress plugin before 2.7.28 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26049	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 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.	4.8	More Details
CVE-2024-4149	The Floating Chat Widget: Contact Chat Icons, WhatsApp, Telegram Chat, Line Messenger, WeChat, Email, SMS, Call Button WordPress plugin before 3.2.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2024-3977	The WordPress Jitsi Shortcode WordPress plugin through 0.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-3992	The Amen WordPress plugin through 3.3.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-4005	The Social Pixel WordPress plugin through 2.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-37828	A stored cross-site scripting (XSS) in Vermeg Agile Reporter v23.2.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Message field under the Set Broadcast Message module.	4.8	More Details
CVE-2024-31159	The parameter used in the certain page of ASUS Download Master is not properly filtered for user input. A remote attacker with administrative privilege can insert JavaScript code to the parameter for Reflected Cross-site scripting attacks.	4.8	More Details
CVE-2024-28970	Dell Client BIOS contains an Out-of-bounds Write vulnerability. A local authenticated malicious user with admin privileges could potentially exploit this vulnerability, leading to platform denial of service.	4.7	More Details
CVE-2024-32904	In ProtocolVsimOperationAdapter() of protocolvsimadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with baseband firmware compromise required. User Interaction is not needed for exploitation.	4.7	More Details
CVE-2024-27179	Admin cookies are written in clear-text in logs. An attacker can retrieve them and bypass the authentication mechanism. As for the affected products/models/versions, see the reference URL.	4.7	More Details
CVE-2024-29778	In ProtocolPsDedicatedBearInfoAdapter::processQosSession of protocolpsadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with baseband firmware compromise required. User interaction is not needed for exploitation.	4.7	More Details
CVE-2024-32898	In ProtocolCellIdentityParserV4::Parse() of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with baseband firmware compromise required. User Interaction is not needed for exploitation.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36977	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: Wait unconditionally after issuing EndXfer command Currently all controller IP/revisions except DWC3_usb3 >= 310a wait 1ms unconditionally for ENDXFER completion when IOC is not set. This is because DWC_usb3 controller revisions >= 3.10a supports GUCTL2[14: Rst_actbitlater] bit which allows polling CMDACT bit to know whether ENDXFER command is completed. Consider a case where an IN request was queued, and parallelly soft_disconnect was called (due to ffs_epfile_release). This eventually calls stop_active_transfer with IOC cleared, hence send_gadget_ep_cmd() skips waiting for CMDACT cleared during EndXfer. For DWC3 controllers with revisions >= 310a, we don't forcefully wait for 1ms either, and we proceed by unmapping the requests. If ENDXFER didn't complete by this time, it leads to SMMU faults since the controller would still be accessing those requests. Fix this by ensuring ENDXFER completion by adding 1ms delay in __dwc3_stop_active_transfer() unconditionally.	4.7	More Details
CVE-2024-6055	Improper removal of sensitive information in data source export feature in Devolutions Remote Desktop Manager 2024.1.32.0 and earlier on Windows allows an attacker that obtains the exported settings to recover powershell credentials configured on the data source via stealing the configuration file.	4.7	More Details
CVE-2024-3754	The Alemha watermarker WordPress plugin through 1.3.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.7	More Details
CVE-2024-37182	Mattermost Desktop App versions <=5.7.0 fail to correctly prompt for permission when opening external URLs which allows a remote attacker to force a victim over the Internet to run arbitrary programs on the victim's system via custom URI schemes.	4.7	More Details
CVE-2024-3993	The AZAN Plugin WordPress plugin through 0.6 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	4.6	More Details
CVE-2024-37317	The Nextcloud Notes app is a distraction free notes taking app for Nextcloud. If an attacker managed to share a folder called `Notes/` with a newly created user before they logged in, the Notes app would use that folder store the personal notes. It is recommended that the Nextcloud Notes app is upgraded to 4.9.3.	4.6	More Details
CVE-2024-37316	Nextcloud Calendar is a calendar app for Nextcloud. Authenticated users could create an event with manipulated attachment data leading to a bad redirect for participants when clicked. It is recommended that the Nextcloud Calendar App is upgraded to 4.6.8 or 4.7.2.	4.6	More Details
CVE-2024-4271	The SVGator WordPress plugin through 1.2.6 does not sanitize SVG file contents, which enables users with at least the author role to SVG with malicious JavaScript to conduct Stored XSS attacks.	4.6	More Details
CVE-2024-38280	An unauthorized user is able to gain access to sensitive data, including credentials, by physically retrieving the hard disk of the product as the data is stored in clear text.	4.6	More Details
CVE-2024-38279	The affected product is vulnerable to an attacker modifying the bootloader by using custom arguments to bypass authentication and gain access to the file system and obtain password hashes.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2218	The LuckyWP Table of Contents WordPress plugin through 2.1.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.6	More Details
CVE-2024-5557	CWE-532: Insertion of Sensitive Information into Log File vulnerability exists that could cause exposure of SNMP credentials when an attacker has access to the controller logs.	4.5	More Details
CVE-2023-52890	NTFS-3G before 75dcdc2 has a use-after-free in ntfs_uppercase_mbs in libntfs-3g/unistr.c. NOTE: discussion suggests that exploitation would be challenging.	4.5	More Details
CVE-2024-37891	urllib3 is a user-friendly HTTP client library for Python. When using urllib3's proxy support with `ProxyManager`, the `Proxy-Authorization` header is only sent to the configured proxy, as expected. However, when sending HTTP requests *without* using urllib3's proxy support, it's possible to accidentally configure the `Proxy-Authorization` header even though it won't have any effect as the request is not using a forwarding proxy or a tunneling proxy. In those cases, urllib3 doesn't treat the `Proxy-Authorization` HTTP header as one carrying authentication material and thus doesn't strip the header on cross-origin redirects. Because this is a highly unlikely scenario, we believe the severity of this vulnerability is low for almost all users. Out of an abundance of caution urllib3 will automatically strip the `Proxy-Authorization` header during cross-origin redirects to avoid the small chance that users are doing this on accident. Users should use urllib3's proxy support or disable automatic redirects to achieve safe processing of the `Proxy-Authorization` header, but we still decided to strip the header by default in order to further protect users who aren't using the correct approach. We believe the number of usages affected by this advisory is low. It requires all of the following to be true to be exploited: 1. Setting the `Proxy-Authorization` header without using urllib3's built-in proxy support. 2. Not disabling HTTP redirects. 3. Either not using an HTTPS origin server or for the proxy or target origin to redirect to a malicious origin. Users are advised to update to either version 1.26.19 or version 2.2.2. Users unable to upgrade may use the `Proxy-Authorization` header with urllib3's `ProxyManager`, disable HTTP redirects using `redirects=False` when sending requests, or not user the `Proxy-Authorization` header as mitigations.	4.4	More Details
CVE-2024-34012	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis Cloud Manager (Windows) before build 6.2.24135.272.	4.4	More Details
CVE-2024-25052	IBM Jazz Reporting Service 7.0.3 stores user credentials in plain clear text which can be read by an admin user. IBM X-Force ID: 283363.	4.4	More Details
CVE-2024-4201	A cross-site scripting issue has been discovered in GitLab affecting all versions starting from 5.1 before 16.10.7, all versions starting from 16.11 before 16.111.4, all versions starting from 17.0 before 17.0.2. When viewing an XML file in a repository in raw mode, it can be made to render as HTML if viewed under specific circumstances.	4.4	More Details
CVE-2024-5553	The Premium Addons for Elementor plugin for WordPress is vulnerable to DOM-Based Stored Cross-Site Scripting via several parameters in all versions up to, and including, 4.10.33 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 and edits an injected element, and subsequently clicks the element with the mouse scroll wheel.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1766	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via a user's Display Name in all versions up to, and including, 3.2.86 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. This vulnerability requires social engineering to successfully exploit, and the impact would be very limited due to the attacker requiring a user to login as the user with the injected payload for execution.	4.4	More Details
CVE-2024-5905	A problem with a protection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local low privileged Windows user to disrupt some functionality of the agent. However, they are not able to disrupt Cortex XDR agent protection mechanisms using this vulnerability.	4.4	More Details
CVE-2024-27175	Remote Command program allows an attacker to read any file using a Local File Inclusion vulnerability. An attacker can read any file on the printer. As for the affected products/models/versions, see the reference URL.	4.4	More Details
CVE-2023-51670	Missing Authorization vulnerability in FunnelKit FunnelKit Checkout.This issue affects FunnelKit Checkout: from n/a through 3.10.3.	4.3	More Details
CVE-2023-6492	The Simple Sitemap – Create a Responsive HTML Sitemap plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.5.13. This is due to missing or incorrect nonce validation in the 'admin_notices' hook found in class-settings.php. This makes it possible for unauthenticated attackers to reset the plugin options to a default state via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-51680	Missing Authorization vulnerability in TechnoVama Quotes for WooCommerce.This issue affects Quotes for WooCommerce: from n/a through 2.0.1.	4.3	More Details
CVE-2023-52117	Missing Authorization vulnerability in Metagauss ProfileGrid.This issue affects ProfileGrid: from n/a through 5.6.6.	4.3	More Details
CVE-2024-0892	The Schema App Structured Data plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.2.0. This is due to missing or incorrect nonce validation on the MarkUpdate function. This makes it possible for unauthenticated attackers to update and delete post metadata via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-51524	Missing Authorization vulnerability in weForms.This issue affects weForms: from n/a through 1.6.18.	4.3	More Details
CVE-2024-5860	The Tickera – WordPress Event Ticketing plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the tc_dl_delete_tickets AJAX action in all versions up to, and including, 3.5.2.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete all tickets associated with events.	4.3	More Details
CVE-2024-37883	Nextcloud Deck is a kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. A user with access to a deck board was able to access comments and attachments of already deleted cards. It is recommended that the Nextcloud Deck app is upgraded to 1.6.6 or 1.7.5 or 1.8.7 or 1.9.6 or 1.11.3 or 1.12.1.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4751	The WP Prayer II WordPress plugin through 2.4.7 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details
CVE-2024-3972	The Similarity WordPress plugin through 3.0 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	4.3	More Details
CVE-2024-38504	In JetBrains YouTrack before 2024.2.34646 the Guest User Account was enabled for attaching files to articles	4.3	More Details
CVE-2024-28969	Dell SCG, versions prior to 5.24.00.00, contain an Improper Access Control vulnerability in the SCG exposed for an internal update REST API (if enabled by Admin user from UI). A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain APIs applicable only for Admin Users on the application's backend database that could potentially allow an unauthorized user access to restricted resources.	4.3	More Details
CVE-2024-32915	In CellInfoListParserV2::FillCellInfo() of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with baseband firmware compromise required. User interaction is not needed for exploitation.	4.3	More Details
CVE-2024-5897	A vulnerability has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /classes/Master.php?f=log_visitor. The manipulation of the argument name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268141 was assigned to this vulnerability.	4.3	More Details
CVE-2023-51523	Missing Authorization vulnerability in WriterSystem WooCommerce Easy Duplicate Product.This issue affects WooCommerce Easy Duplicate Product: from n/a through 0.3.0.7.	4.3	More Details
CVE-2024-2023	The Folders and Folders Pro plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 3.0 in Folders and 3.0.2 in Folders Pro via the 'handle_folders_file_upload' function. This makes it possible for authenticated attackers, with author access and above, to upload files to arbitrary locations on the server.	4.3	More Details
CVE-2023-51376	Missing Authorization vulnerability in Brainstorm Force ProjectHuddle Client Site.This issue affects ProjectHuddle Client Site: from n/a through 1.0.34.	4.3	More Details
CVE-2023-35045	Missing Authorization vulnerability in Fat Rat Fat Rat Collect.This issue affects Fat Rat Collect: from n/a through 2.6.7.	4.3	More Details
CVE-2024-37279	A flaw was discovered in Kibana, allowing view-only users of alerting to use the run_soon API making the alerting rule run continuously, potentially affecting the system availability if the alerting rule is running complex queries.	4.3	More Details
CVE-2024-6108	A vulnerability was found in Genexis Tilgin Home Gateway 322_AS0500-03_05_13_05. It has been classified as problematic. Affected is an unknown function of the file /vood/cgi-bin/vood_view.cgi?act=index&lang=EN# of the component Login. The manipulation of the argument errmsg leads to basic cross site scripting. It is possible to launch the attack remotely. VDB-268854 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51526	Missing Authorization vulnerability in Brett Shumaker Simple Staff List.This issue affects Simple Staff List: from n/a through 2.2.4.	4.3	More Details
CVE-2024-3971	The Similarity WordPress plugin through 3.0 does not have CSRF check in place when resetting its settings, which could allow attackers to make a logged in admin reset them via a CSRF attack	4.3	More Details
CVE-2024-5858	The AI Infographic Maker plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the qcld_openai_title_generate_desc AJAX action in all versions up to, and including, 4.7.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary post titles.	4.3	More Details
CVE-2023-47845	Cross-Site Request Forgery (CSRF) vulnerability in Lim Kai Yang Grab & Save.This issue affects Grab & Save: from n/a through 1.0.4.	4.3	More Details
CVE-2024-38083	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4.3	More Details
CVE-2024-36589	An issue in Annonshop.app DecentralizeJustice/anonymousLocker commit 2b2b4 to ba9fd and DecentralizeJustice/anonBackend commit 57837 to cd815 was discovered to store credentials in plaintext.	4.3	More Details
CVE-2024-38313	In certain scenarios a malicious website could attempt to display a fake location URL bar which could mislead users as to the actual website address This vulnerability affects Firefox for iOS < 127.	4.3	More Details
CVE-2023-25030	Missing Authorization vulnerability in Buy Me a Coffee.This issue affects Buy Me a Coffee: from n/a through 3.7.	4.3	More Details
CVE-2023-47828	Missing Authorization vulnerability in Mandrill wpMandrill.This issue affects wpMandrill: from n/a through 1.33.	4.3	More Details
CVE-2023-44234	Missing Authorization vulnerability in Bastianon Massimo WP GPX Map.This issue affects WP GPX Map: from n/a through 1.7.08.	4.3	More Details
CVE-2024-38394	Mismatches in interpreting USB authorization policy between GNOME Settings Daemon (GSD) through 46.0 and the Linux kernel's underlying device matching logic allow a physically proximate attacker to access some unintended Linux kernel USB functionality, such as USB device-specific kernel modules and filesystem implementations. NOTE: the GSD supplier indicates that consideration of a mitigation for this within GSD would be in the context of "a new feature, not a CVE."	4.3	More Details
CVE-2024-5891	A vulnerability was found in Quay. If an attacker can obtain the client ID for an application, they can use an OAuth token to authenticate despite not having access to the organization from which the application was created. This issue is limited to authentication and not authorization. However, in configurations where endpoints rely only on authentication, a user may authenticate to applications they otherwise have no access to.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37663	Redmi router RB03 v1.0.57 is vulnerable to forged ICMP redirect message attacks. An attacker in the same WLAN as the victim can hijack the traffic between the victim and any remote server by sending out forged ICMP redirect messages.	4.1	More Details
CVE-2024-4176	An Cross site scripting vulnerability in the EDR XConsole before this release allowed an attacker to potentially leverage an XSS/HTML-Injection using command line variables. A malicious threat actor could execute commands on the victim's browser for sending carefully crafted malicious links to the EDR XConsole end user.	4.1	More Details
CVE-2024-5464	Vulnerability of insufficient permission verification in the NearLink module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.0	More Details
CVE-2024-32923	there is a possible cellular denial of service due to a logic error in the code. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	4.0	More Details
CVE-2024-37885	The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server with your computer. A code injection in Nextcloud Desktop Client for macOS allowed to load arbitrary code when starting the client with DYLD_INSERT_LIBRARIES set in the enviroment. It is recommended that the Nextcloud Desktop client is upgraded to 3.12.0.	3.8	More Details
CVE-2024-36287	Mattermost Desktop App versions <=5.7.0 fail to disable certain Electron debug flags which allows for bypassing TCC restrictions on macOS.	3.8	More Details
CVE-2024-30119	HCL DRYiCE Optibot Reset Station is impacted by a missing Strict Transport Security Header. This could allow an attacker to intercept or manipulate data during redirection.	3.7	More Details
CVE-2024-6056	A vulnerability was found in nasirkhan Laravel Starter up to 11.8.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /forgot-password of the component Password Reset Handler. The manipulation of the argument Email leads to observable response 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 identifier of this vulnerability is VDB-268784. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2023-49559	An issue in vektah gqlparser open-source-library v.2.5.10 allows a remote attacker to cause a denial of service via a crafted script to the parserDirectives function.	3.7	More Details
CVE-2024-6129	A vulnerability, which was classified as problematic, was found in spa-cartcms 1.9.0.6. Affected is an unknown function of the file /login of the component Username Handler. The manipulation of the argument email leads to observable behavioral discrepancy. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-268896.	3.7	More Details
CVE-2024-37314	Nextcloud Photos is a photo management app. Users can remove photos from the album of registered users. It is recommended that the Nextcloud Server is upgraded to 25.0.7 or 26.0.2 and the Nextcloud Enterprise Server is upgraded to 25.0.7 or 26.0.2.	3.5	More Details
CVE-2024-38507	In JetBrains Hub before 2024.2.34646 stored XSS via project description was possible	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1891	A stored cross site scripting vulnerability exists in Tenable Security Center where an authenticated, remote attacker could inject HTML code into a web application scan result page.	3.5	More Details
CVE-2024-6005	A vulnerability was found in ZKTeco ZKBio CVSecurity V5000 4.1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Department Section. The manipulation of the argument Department Name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268693 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-37887	Nextcloud Server is a self hosted personal cloud system. Private shared calendar events' recurrence exceptions can be read by sharees. It is recommended that the Nextcloud Server is upgraded to 27.1.10 or 28.0.6 or 29.0.1 and that the Nextcloud Enterprise Server is upgraded to 27.1.10 or 28.0.6 or 29.0.1.	3.5	More Details
CVE-2024-36226	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect the integrity of the page. Exploitation of this issue requires user interaction.	3.5	More Details
CVE-2024-37315	Nextcloud Server is a self hosted personal cloud system. An attacker with read-only access to a file is able to restore older versions of a document when the files_versions app is enabled. It is recommended that the Nextcloud Server is upgraded to 26.0.12, 27.1.7 or 28.0.3 and that the Nextcloud Enterprise Server is upgraded to 23.0.12.16, 24.0.12.12, 25.0.13.6, 26.0.12, 27.1.7 or 28.0.3.	3.5	More Details
CVE-2024-37158	Evmos is the Ethereum Virtual Machine (EVM) Hub on the Cosmos Network. Preliminary checks on actions computed by the clawback vesting accounts are performed in the ante handler. Evmos core, implements two different ante handlers: one for Cosmos transactions and one for Ethereum transactions. Checks performed on the two implementation are different. The vulnerability discovered allowed a clawback account to bypass Cosmos ante handler checks by sending an Ethereum transaction targeting a precompile used to interact with a Cosmos SDK module. This vulnerability is fixed in 18.0.0.	3.5	More Details
CVE-2024-37884	Nextcloud Server is a self hosted personal cloud system. A malicious user was able to send delete requests for old versions of files they only got shared with read permissions. It is recommended that the Nextcloud Server is upgraded to 26.0.12 or 27.1.7 or 28.0.3 and that the Nextcloud Enterprise Server is upgraded to 26.0.12 or 27.1.7 or 28.0.3.	3.5	More Details
CVE-2024-6006	A vulnerability was found in ZKTeco ZKBio CVSecurity V5000 4.1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Summer Schedule Handler. The manipulation of the argument Schedule Name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-268694 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-37159	Evmos is the Ethereum Virtual Machine (EVM) Hub on the Cosmos Network. This vulnerability allowed a user to create a validator using vested tokens to deposit the self-bond. This vulnerability is fixed in 18.0.0.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26126	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect the integrity of the page. Exploitation of this issue requires user interaction.	3.5	More Details
CVE-2024-6058	A vulnerability classified as problematic has been found in LabVantage LIMS 2017. This affects an unknown part of the file /labvantage/rc?command=page&page=SampleHistoricalList&_iframename=list&__crc=crc_1701669816260. The manipulation of the argument height/width leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-268785 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-26127	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect the integrity of the page. Exploitation of this issue requires user interaction.	3.5	More Details
CVE-2024-22333	IBM Maximo Asset Management 7.6.1.3 and IBM Maximo Application Suite 8.10 and 8.11 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 279973.	3.3	More Details
CVE-2024-6061	A vulnerability has been found in GPAC 2.5-DEV-rev228-g11067ea92-master and classified as problematic. Affected by this vulnerability is the function isoffin_process of the file src/filters/isoffin_read.c of the component MP4Box. The manipulation leads to infinite loop. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The identifier of the patch is 20c0f29139a82779b86453ce7f68d0681ec7624c. It is recommended to apply a patch to fix this issue. The identifier VDB-268789 was assigned to this vulnerability.	3.3	More Details
CVE-2024-6062	A vulnerability was found in GPAC 2.5-DEV-rev228-g11067ea92-master and classified as problematic. Affected by this issue is the function swf_svg_add_iso_sample of the file src/filters/load_text.c of the component MP4Box. The manipulation leads to null pointer dereference. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The patch is identified as 31e499d310a48bd17c8b055a0bfe0fe35887a7cd. It is recommended to apply a patch to fix this issue. VDB-268790 is the identifier assigned to this vulnerability.	3.3	More Details
CVE-2024-31870	IBM Db2 for i 7.2, 7.3, 7.4, and 7.5 supplies user defined table function is vulnerable to user enumeration by a local authenticated attacker, without having authority to the related *USRPRF objects. This can be used by a malicious actor to gather information about users that can be targeted in further attacks. IBM X-Force ID: 287174.	3.3	More Details
CVE-2024-6063	A vulnerability was found in GPAC 2.5-DEV-rev228-g11067ea92-master. It has been classified as problematic. This affects the function m2tsdmx_on_event of the file src/filters/dmx_m2ts.c of the component MP4Box. The manipulation leads to null pointer dereference. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The patch is named 8767ed0a77c4b02287db3723e92c2169f67c85d5. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-268791.	3.3	More Details
CVE-2024-5469	DoS in KAS in GitLab CE/EE affecting all versions from 16.10.0 prior to 16.10.6 and 16.11.0 prior to 16.11.3 allows an attacker to crash KAS via crafted gRPC requests.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30120	HCL DRYiCE Optibot Reset Station is impacted by an Unused Parameter in the web application.	2.9	More Details
CVE-2024-3073	The Easy WP SMTP by SendLayer – WordPress SMTP and Email Log Plugin plugin for WordPress is vulnerable to information exposure in all versions up to, and including, 2.3.0. This is due to plugin providing the SMTP password in the SMTP Password field when viewing the settings. This makes it possible for authenticated attackers, with administrative-level access and above, to view the SMTP password for the supplied server. Although this would not be useful for attackers in most cases, if an administrator account becomes compromised this could be useful information to an attacker in a limited environment.	2.7	More Details
CVE-2024-5967	A vulnerability was found in Keycloak. The LDAP testing endpoint allows changing the Connection URL independently without re-entering the currently configured LDAP bind credentials. This flaw allows an attacker with admin access (permission manage-realm) to change the LDAP host URL ("Connection URL") to a machine they control. The Keycloak server will connect to the attacker's host and try to authenticate with the configured credentials, thus leaking them to the attacker. As a consequence, an attacker who has compromised the admin console or compromised a user with sufficient privileges can leak domain credentials and attack the domain.	2.7	More Details
CVE-2024-5798	Vault and Vault Enterprise did not properly validate the JSON Web Token (JWT) role-bound audience claim when using the Vault JWT auth method. This may have resulted in Vault validating a JWT the audience and role-bound claims do not match, allowing an invalid login to succeed when it should have been rejected. This vulnerability, CVE-2024-5798, was fixed in Vault and Vault Enterprise 1.17.0, 1.16.3, and 1.15.9	2.6	More Details
CVE-2024-6059	A vulnerability, which was classified as problematic, has been found in Ingenico Estate Manager 2023. This issue affects some unknown processing of the file /emgui/rest/ums/messages of the component News Feed. The manipulation of the argument message leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268787. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2024-6082	A vulnerability, which was classified as problematic, has been found in PHPVibe 11.0.46. This issue affects some unknown processing of the file functionalities.global.php of the component Global Options Page. The manipulation of the argument site-logo-text leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-268823. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2024-29181	Strapi is an open-source content management system. Prior to version 4.19.1, a super admin can create a collection where an item in the collection has an association to another collection. When this happens, another user with Author Role can see the list of associated items they did not create. They should see nothing but their own items they created not all items ever created. Users should upgrade @strapi/plugin-content-manager to version 4.19.1 to receive a patch.	2.3	More Details
CVE-2024-36974	In the Linux kernel, the following vulnerability has been resolved: net/sched: taprio: always validate TCA_TAPRIO_ATTR_PRIOMAP If one TCA_TAPRIO_ATTR_PRIOMAP attribute has been provided, taprio_parse_mqprio_opt() must validate it, or userspace can inject arbitrary data to the kernel, the second time taprio_change() is called. First call (with valid attributes) sets dev->num_tc to a non zero value. Second call (with arbitrary mqprio attributes) returns early from taprio_parse_mqprio_opt() and bad things can happen.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5996	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-2230	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-38285	Logs storing credentials are insufficiently protected and can be decoded through the use of open source tools.	N/A	More Details
CVE-2024-35328	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2024-6046	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-5203	Rejected reason: After careful review of CVE-2024-5203, it has been determined that the issue is not exploitable in real-world scenarios. Moreover, the exploit assumes that the attacker has access to a session code parameter that matches a cookie on the Keycloak server. However the attacker does not have access to the cookie, and can therefore not craft a malicious request.	N/A	More Details
CVE-2024-36459	A CRLF cross-site scripting vulnerability has been identified in certain configurations of the SiteMinder Web Agent for IIS Web Server and SiteMinder Web Agent for Domino Web Server. As a result, an attacker can execute arbitrary Javascript code in a client browser.	N/A	More Details
CVE-2024-36699	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2024-4315	parisneo/lollms version 9.5 is vulnerable to Local File Inclusion (LFI) attacks due to insufficient path sanitization. The `sanitize_path_from_endpoint` function fails to properly sanitize Windows-style paths (backward slash `\`), allowing attackers to perform directory traversal attacks on Windows systems. This vulnerability can be exploited through various routes, including `personalities` and `/del_preset`, to read or delete any file on the Windows filesystem, compromising the system's availability.	N/A	More Details
CVE-2024-32924	In DeregAcceptProcINT of cn_NrmmStateDeregInit.cpp, there is a possible denial of service due to a logic error in the code. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A	More Details
CVE-2024-36975	In the Linux kernel, the following vulnerability has been resolved: KEYS: trusted: Do not use WARN when encode fails When asn1_encode_sequence() fails, WARN is not the correct solution. 1. asn1_encode_sequence() is not an internal function (located in lib/asn1_encode.c). 2. Location is known, which makes the stack trace useless. 3. Results a crash if panic_on_warn is set. It is also noteworthy that the use of WARN is undocumented, and it should be avoided unless there is a carefully considered rationale to use it. Replace WARN with pr_err, and print the return value instead, which is only useful piece of information.	N/A	More Details
CVE-2024-38282	Utilizing default credentials, an attacker is able to log into the camera's operating system which could allow changes to be made to the operations or shutdown the camera requiring a physical reboot of the system.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5211	A path traversal vulnerability in mintplex-labs/anything-llm allowed a manager to bypass the `normalizePath()` function, intended to defend against path traversal attacks. This vulnerability enables the manager to read, delete, or overwrite the 'anythingllm.db' database file and other files stored in the 'storage' directory, such as internal communication keys and .env secrets. Exploitation of this vulnerability could lead to application compromise, denial of service (DoS) attacks, and unauthorized admin account takeover. The issue stems from improper validation of user-supplied input in the process of setting a custom logo for the app, which can be manipulated to achieve arbitrary file read, deletion, or overwrite, and to execute a DoS attack by deleting critical files required for the application's operation.	N/A	More Details
CVE-2024-5961	Improper neutralization of input during web page generation vulnerability in 2ClickPortal software allows reflected cross-site scripting (XSS). An attacker might trick somebody into using a crafted URL, which will cause a script to be run in user's browser. This issue affects 2ClickPortal software versions from 7.2.31 through 7.6.4.	N/A	More Details
CVE-2024-38283	Sensitive customer information is stored in the device without encryption.	N/A	More Details
CVE-2024-35325	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2024-37369	A privilege escalation vulnerability exists in the affected product. The vulnerability allows low-privilege users to edit scripts, bypassing Access Control Lists, and potentially gaining further access within the system.	N/A	More Details
CVE-2024-21685	This High severity Information Disclosure vulnerability was introduced in versions 9.4.0, 9.12.0, and 9.15.0 of Jira Core Data Center. This Information Disclosure vulnerability, with a CVSS Score of 7.4, allows an unauthenticated attacker to view sensitive information via an Information Disclosure vulnerability which has high impact to confidentiality, no impact to integrity, no impact to availability, and requires user interaction. Atlassian recommends that Jira Core Data Center customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Jira Core Data Center 9.4: Upgrade to a release greater than or equal to 9.4.21 Jira Core Data Center 9.12: Upgrade to a release greater than or equal to 9.12.8 Jira Core Data Center 9.16: Upgrade to a release greater than or equal to 9.16.0 See the release notes. You can download the latest version of Jira Core Data Center from the download center. This vulnerability was found internally.	N/A	More Details
CVE-2024-38284	Transmitted data is logged between the device and the backend service. An attacker could use these logs to perform a replay attack to replicate calls.	N/A	More Details
CVE-2024-5783	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2021-4237	Rejected reason: reserved but not needed	N/A	More Details
CVE-2024-3468	There is a vulnerability in AVEVA PI Web API that could allow malicious code to execute on the PI Web API environment under the privileges of an interactive user that was socially engineered to use API XML import functionality with content supplied by an attacker.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5782	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-5659	Rockwell Automation was made aware of a vulnerability that causes all affected controllers on the same network to result in a major nonrecoverable fault(MNRF/Assert). This vulnerability could be exploited by sending abnormal packets to the mDNS port. If exploited, the availability of the device would be compromised.	N/A	More Details
CVE-2024-5781	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-5873	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-5780	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-4480	The WP Prayer II WordPress plugin through 2.4.7 does not have CSRF check in place when updating its email settings, which could allow attackers to make a logged in admin change them via a CSRF attack	N/A	More Details
CVE-2024-5927	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-36973	In the Linux kernel, the following vulnerability has been resolved: misc: microchip: pci1xxxx: fix double free in the error handling of gp_aux_bus_probe() When auxiliary_device_add() returns error and then calls auxiliary_device_uninit(), callback function gp_auxiliary_device_release() calls ida_free() and kfree(aux_device_wrapper) to free memory. We should't call them again in the error handling path. Fix this by skipping the redundant cleanup functions.	N/A	More Details
CVE-2024-5899	When Bazel Plugin in intellij imports a project (either using "import project" or "Auto import") the dialog for trusting the project is not displayed. This comes from the fact that both call the method ProjectBuilder.createProject which then calls ProjectManager.getInstance().createProject. This method, as its name suggests is intended to create a new project, not to import an existing one. We recommend upgrading to version 2024.06.04.0.2 or beyond for the IntelliJ, CLion and Android Studio Bazel plugins.	N/A	More Details
CVE-2024-1469	Rejected reason: ** REJECT ** Duplicate assignment. Please use CVE-2024-0845 instead.	N/A	More Details
CVE-2024-37368	A user authentication vulnerability exists in the Rockwell Automation FactoryTalk® View SE. The vulnerability allows a user from a remote system with FTView to send a packet to the customer's server to view an HMI project. Due to the lack of proper authentication, this action is allowed without proper authentication verification.	N/A	More Details
CVE-2024-5779	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5778	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-5777	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-5776	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-2875	Rejected reason: ** REJECT ** Duplicate reservation. Please use CVE-2024-4258 instead.	N/A	More Details
CVE-2024-5934	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-5750	Rejected reason: ** REJECT ** Not a valid security issue.	N/A	More Details
CVE-2024-35326	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details