SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 12 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-2024-35746	Unrestricted Upload of File with Dangerous Type vulnerability in Asghar Hatampoor BuddyPress Cover allows Code Injection.This issue affects BuddyPress Cover: from n/a through 2.1.4.2.	10.0	More Details
CVE-2024-36412	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in events response entry point allows for a SQL injection attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	10.0	More Details
CVE-2024-2013	An authentication bypass vulnerability exists in the FOXMAN-UN/UNEM server / API Gateway component that if exploited allows attackers without any access to interact with the services and the post-authentication attack surface.	10.0	More Details
CVE-2024-5675	Untrusted data deserialization vulnerability has been found in Mentor - Employee Portal, affecting version 3.83.35. This vulnerability could allow an attacker to execute arbitrary code, by injecting a malicious payload into the “ViewState” field.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3549	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to SQL Injection via the 'b2sSortPostType' parameter in all versions up to, and including, 7.4.1 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 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.	9.9	More Details
CVE-2024-34762	Vulnerability discovered by executing a planned security audit. Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WPENGINE INC Advanced Custom Fields PRO allows PHP Local File Inclusion.This issue affects Advanced Custom Fields PRO: from n/a before 6.2.10.	9.9	More Details
CVE-2024-36393	SysAid - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	9.9	More Details
CVE-2024-3592	The Quiz And Survey Master – Best Quiz, Exam and Survey Plugin for WordPress plugin for WordPress is vulnerable to SQL Injection via the 'question_id' parameter in all versions up to, and including, 9.0.1 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.	9.9	More Details
CVE-2024-37301	Document Merge Service is a document template merge service providing an API to manage templates and merge them with given data. Versions 6.5.1 and prior are vulnerable to remote code execution via server-side template injection which, when executed as root, can result in full takeover of the affected system. As of time of publication, no patched version exists, nor have any known workarounds been disclosed.	9.9	More Details
CVE-2024-4295	The Email Subscribers by Icegram Express plugin for WordPress is vulnerable to SQL Injection via the ‘hash’ parameter in all versions up to, and including, 5.7.20 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1228	Use of hard-coded password to the patients' database allows an attacker to retrieve sensitive data stored in the database. The password is the same among all Eurosoft Przychodnia installations. This issue affects Eurosoft Przychodnia software before version 20240417.001 (from that version vulnerability is fixed).	9.8	More Details
CVE-2024-4620	The ARForms - Premium WordPress Form Builder Plugin WordPress plugin before 6.6 allows unauthenticated users to modify uploaded files in such a way that PHP code can be uploaded when an upload file input is included on a form	9.8	More Details
CVE-2024-30163	Invision Community before 4.7.16 allow SQL injection via the applications/nexus/modules/front/store/store.php IPS\nexus\modules\front\store_store::_categoryView() method, where user input passed through the filter request parameter is not properly sanitized before being used to execute SQL queries. This can be exploited by unauthenticated attackers to carry out Blind SQL Injection attacks.	9.8	More Details
CVE-2024-4146	In lunary-ai/lunary version v1.2.13, an incorrect authorization vulnerability exists that allows unauthorized users to access and manipulate projects within an organization they should not have access to. Specifically, the vulnerability is located in the `checkProjectAccess` method within the authorization middleware, which fails to adequately verify if a user has the correct permissions to access a specific project. Instead, it only checks if the user is part of the organization owning the project, overlooking the necessary check against the `account_project` table for explicit project access rights. This flaw enables attackers to gain complete control over all resources within a project, including the ability to create, update, read, and delete any resource, compromising the privacy and security of sensitive information.	9.8	More Details
CVE-2024-37385	Roundcube Webmail before 1.5.7 and 1.6.x before 1.6.7 on Windows allows command injection via im_convert_path and im_identify_path. NOTE: this issue exists because of an incomplete fix for CVE-2020-12641.	9.8	More Details
CVE-2024-31244	Missing Authorization vulnerability in Bricksforge.This issue affects Bricksforge: from n/a through 2.0.17.	9.8	More Details
CVE-2024-4577	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5262	Files or Directories Accessible to External Parties vulnerability in smb server in ProjectDiscovery Interactsh allows remote attackers to read/write any files in the directory and subdirectories of where the victim runs interactsh-server via anonymous login.	9.8	More Details
CVE-2024-3699	Use of hard-coded password to the patients' database allows an attacker to retrieve sensitive data stored in the database. The password is the same among all drEryk Gabinet installations.This issue affects drEryk Gabinet software versions from 7.0.0.0 through 9.17.0.0.	9.8	More Details
CVE-2024-3700	Use of hard-coded password to the patients' database allows an attacker to retrieve sensitive data stored in the database. The password is the same among all Simple Care software installations. This issue affects Estomed Sp. z o.o. Simple Care software in all versions. The software is no longer supported.	9.8	More Details
CVE-2024-4320	A remote code execution (RCE) vulnerability exists in the '/install_extension' endpoint of the parisneo/lollms-webui application, specifically within the `@router.post("/install_extension")` route handler. The vulnerability arises due to improper handling of the `name` parameter in the `ExtensionBuilder().build_extension()` method, which allows for local file inclusion (LFI) leading to arbitrary code execution. An attacker can exploit this vulnerability by crafting a malicious `name` parameter that causes the server to load and execute a `__init__.py` file from an arbitrary location, such as the upload directory for discussions. This vulnerability affects the latest version of parisneo/lollms-webui and can lead to remote code execution without requiring user interaction, especially when the application is exposed to an external endpoint or operated in headless mode.	9.8	More Details
CVE-2024-37014	Langflow through 0.6.19 allows remote code execution if untrusted users are able to reach the "POST /api/v1/custom_component" endpoint and provide a Python script.	9.8	More Details
CVE-2024-36360	OS command injection vulnerability exists in awkblog v0.0.1 (commit hash:7b761b192d0e0dc3eef0f30630e00ece01c8d552) and earlier. If a remote unauthenticated attacker sends a specially crafted HTTP request, an arbitrary OS command may be executed with the privileges of the affected product on the machine running the product.	9.8	More Details
CVE-2024-5695	If an out-of-memory condition occurs at a specific point using allocations in the probabilistic heap checker, an assertion could have been triggered, and in rarer situations, memory corruption could have occurred. This vulnerability affects Firefox < 127.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5699	In violation of spec, cookie prefixes such as `__Secure` were being ignored if they were not correctly capitalized - by spec they should be checked with a case-insensitive comparison. This could have resulted in the browser not correctly honoring the behaviors specified by the prefix. This vulnerability affects Firefox < 127.	9.8	More Details
CVE-2024-5701	Memory safety bugs present in Firefox 126. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 127.	9.8	More Details
CVE-2024-30080	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	9.8	More Details
CVE-2024-22074	Dynamsoft Service 1.8.1025 through 1.8.2013, 1.7.0330 through 1.7.2531, 1.6.0428 through 1.6.1112, 1.5.0625 through 1.5.3116, 1.4.0618 through 1.4.1230, and 1.0.516 through 1.3.0115 has Incorrect Access Control. This is fixed in 1.8.2014, 1.7.4212, 1.6.3212, 1.5.31212, 1.4.3212, and 1.3.3212.	9.8	More Details
CVE-2024-36673	Sourcecodester Pharmacy/Medical Store Point of Sale System 1.0 is vulnerable SQL Injection via login.php. This vulnerability stems from inadequate validation of user inputs for the email and password parameters, allowing attackers to inject malicious SQL queries.	9.8	More Details
CVE-2024-3429	A path traversal vulnerability exists in the parisneo/lollms application, specifically within the `sanitize_path_from_endpoint` and `sanitize_path` functions in `lollms_core\lollms\security.py`. This vulnerability allows for arbitrary file reading when the application is running on Windows. The issue arises due to insufficient sanitization of user-supplied input, enabling attackers to bypass the path traversal protection mechanisms by crafting malicious input. Successful exploitation could lead to unauthorized access to sensitive files, information disclosure, and potentially a denial of service (DoS) condition by including numerous large or resource-intensive files. This vulnerability affects the latest version prior to 9.6.	9.8	More Details
CVE-2024-36779	Sourcecodester Stock Management System v1.0 is vulnerable to SQL Injection via editCategories.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3104	A remote code execution vulnerability exists in mintplex-labs/anything-llm due to improper handling of environment variables. Attackers can exploit this vulnerability by injecting arbitrary environment variables via the `POST /api/system/update-env` endpoint, which allows for the execution of arbitrary code on the host running anything-llm. The vulnerability is present in the latest version of anything-llm, with the latest commit identified as fde905aac1812b84066ff72e5f2f90b56d4c3a59. This issue has been fixed in version 1.0.0. Successful exploitation could lead to code execution on the host, enabling attackers to read and modify data accessible to the user running the service, potentially leading to a denial of service.	9.8	More Details
CVE-2024-5452	A remote code execution (RCE) vulnerability exists in the lightning-ai/pytorch-lightning library version 2.2.1 due to improper handling of deserialized user input and mismanagement of dunder attributes by the `deepdiff` library. The library uses `deepdiff.Delta` objects to modify application state based on frontend actions. However, it is possible to bypass the intended restrictions on modifying dunder attributes, allowing an attacker to construct a serialized delta that passes the deserializer whitelist and contains dunder attributes. When processed, this can be exploited to access other modules, classes, and instances, leading to arbitrary attribute write and total RCE on any self-hosted pytorch-lightning application in its default configuration, as the delta endpoint is enabled by default.	9.8	More Details
CVE-2024-5482	A Server-Side Request Forgery (SSRF) vulnerability exists in the 'add_webpage' endpoint of the parisneo/lollms-webui application, affecting the latest version. The vulnerability arises because the application does not adequately validate URLs entered by users, allowing them to input arbitrary URLs, including those that target internal resources such as 'localhost' or '127.0.0.1'. This flaw enables attackers to make unauthorized requests to internal or external systems, potentially leading to access to sensitive data, service disruption, network integrity compromise, business logic manipulation, and abuse of third-party resources. The issue is critical and requires immediate attention to maintain the application's security and integrity.	9.8	More Details
CVE-2024-1881	AutoGPT, a component of significant-gravitas/autogpt, is vulnerable to an improper neutralization of special elements used in an OS command ('OS Command Injection') due to a flaw in its shell command validation function. Specifically, the vulnerability exists in versions v0.5.0 up to but not including 5.1.0. The issue arises from the application's method of validating shell commands against an allowlist or denylist, where it only checks the first word of the command. This allows an attacker to bypass the intended restrictions by crafting commands that are executed despite not being on the allowlist or by including malicious commands not present in the denylist. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary shell commands.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36736	An issue in the oneflow.permute component of OneFlow-Inc. Oneflow v0.9.1 causes an incorrect calculation when the same dimension operation is performed.	9.8	More Details
CVE-2024-2359	A vulnerability in the parisneo/lollms-webui version 9.3 allows attackers to bypass intended access restrictions and execute arbitrary code. The issue arises from the application's handling of the `/execute_code` endpoint, which is intended to be blocked from external access by default. However, attackers can exploit the `/update_setting` endpoint, which lacks proper access control, to modify the `host` configuration at runtime. By changing the `host` setting to an attacker-controlled value, the restriction on the `/execute_code` endpoint can be bypassed, leading to remote code execution. This vulnerability is due to improper neutralization of special elements used in an OS command (`Improper Neutralization of Special Elements used in an OS Command`).	9.8	More Details
CVE-2024-2360	parisneo/lollms-webui is vulnerable to path traversal attacks that can lead to remote code execution due to insufficient sanitization of user-supplied input in the 'Database path' and 'PDF LaTeX path' settings. An attacker can exploit this vulnerability by manipulating these settings to execute arbitrary code on the targeted server. The issue affects the latest version of the software. The vulnerability stems from the application's handling of the 'discussion_db_name' and 'pdf_latex_path' parameters, which do not properly validate file paths, allowing for directory traversal. This vulnerability can also lead to further file exposure and other attack vectors by manipulating the 'discussion_db_name' parameter.	9.8	More Details
CVE-2024-34832	Directory Traversal vulnerability in CubeCart v.6.5.5 and before allows an attacker to execute arbitrary code via a crafted file uploaded to the _g and node parameters.	9.8	More Details
CVE-2024-5171	Integer overflow in libaom internal function img_alloc_helper can lead to heap buffer overflow. This function can be reached via 3 callers: * Calling aom_img_alloc() with a large value of the d_w, d_h, or align parameter may result in integer overflows in the calculations of buffer sizes and offsets and some fields of the returned aom_image_t struct may be invalid. * Calling aom_img_wrap() with a large value of the d_w, d_h, or align parameter may result in integer overflows in the calculations of buffer sizes and offsets and some fields of the returned aom_image_t struct may be invalid. * Calling aom_img_alloc_with_border() with a large value of the d_w, d_h, align, size_align, or border parameter may result in integer overflows in the calculations of buffer sizes and offsets and some fields of the returned aom_image_t struct may be invalid.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2624	A path traversal and arbitrary file upload vulnerability exists in the parisneo/lollms-webui application, specifically within the `@router.get("/switch_personal_path")` endpoint in `./lollms-webui/lollms_core/lollms/server/endpoints/lollms_user.py`. The vulnerability arises due to insufficient sanitization of user-supplied input for the `path` parameter, allowing an attacker to specify arbitrary file system paths. This flaw enables direct arbitrary file uploads, leakage of `personal_data`, and overwriting of configurations in `lollms-webui`->`configs` by exploiting the same named directory in `personal_data`. The issue affects the latest version of the application and is fixed in version 9.4. Successful exploitation could lead to sensitive information disclosure, unauthorized file uploads, and potentially remote code execution by overwriting critical configuration files.	9.8	More Details
CVE-2024-3234	The gaizhenbiao/chuanhuchatgpt application is vulnerable to a path traversal attack due to its use of an outdated gradio component. The application is designed to restrict user access to resources within the `web_assets` folder. However, the outdated version of gradio it employs is susceptible to path traversal, as identified in CVE-2023-51449. This vulnerability allows unauthorized users to bypass the intended restrictions and access sensitive files, such as `config.json`, which contains API keys. The issue affects the latest version of chuanhuchatgpt prior to the fixed version released on 20240305.	9.8	More Details
CVE-2024-3322	A path traversal vulnerability exists in the 'cyber_security/codeguard' native personality of the parisneo/lollms-webui, affecting versions up to 9.5. The vulnerability arises from the improper limitation of a pathname to a restricted directory in the 'process_folder' function within 'lollms-webui/zoos/personalities_zoo/cyber_security/codeguard/scripts/processor.py'. Specifically, the function fails to properly sanitize user-supplied input for the 'code_folder_path', allowing an attacker to specify arbitrary paths using '../' or absolute paths. This flaw leads to arbitrary file read and overwrite capabilities in specified directories without limitations, posing a significant risk of sensitive information disclosure and unauthorized file manipulation.	9.8	More Details
CVE-2024-24790	The various Is methods (IsPrivate, IsLoopback, etc) did not work as expected for IPv4-mapped IPv6 addresses, returning false for addresses which would return true in their traditional IPv4 forms.	9.8	More Details
CVE-2024-4743	The LifterLMS – WordPress LMS Plugin for eLearning plugin for WordPress is vulnerable to SQL Injection via the orderBy attribute of the lifterlms_favorites shortcode in all versions up to, and including, 7.6.2 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.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3408	man-group/dtale version 3.10.0 is vulnerable to an authentication bypass and remote code execution (RCE) due to improper input validation. The vulnerability arises from a hardcoded `SECRET_KEY` in the flask configuration, allowing attackers to forge a session cookie if authentication is enabled. Additionally, the application fails to properly restrict custom filter queries, enabling attackers to execute arbitrary code on the server by bypassing the restriction on the `/update-settings` endpoint, even when `enable_custom_filters` is not enabled. This vulnerability allows attackers to bypass authentication mechanisms and execute remote code on the server.	9.8	More Details
CVE-2024-36408	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in the `Alerts` controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	9.6	More Details
CVE-2024-4008	FDSK Leak in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to take control via access to local KNX Bus-System	9.6	More Details
CVE-2024-36411	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in EmailUIAjax displayView controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	9.6	More Details
CVE-2024-36410	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in EmailUIAjax messages count controller. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	9.6	More Details
CVE-2024-36409	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, poor input validation allows for SQL Injection in Tree data entry point. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35225	Jupyter Server Proxy allows users to run arbitrary external processes alongside their notebook server and provide authenticated web access to them. Versions of 3.x prior to 3.2.4 and 4.x prior to 4.2.0 have a reflected cross-site scripting (XSS) issue. The `/proxy` endpoint accepts a `host` path segment in the format `/proxy/<host>`. When this endpoint is called with an invalid `host` value, `jupyter-server-proxy` replies with a response that includes the value of `host`, without sanitization [2]. A third-party actor can leverage this by sending a phishing link with an invalid `host` value containing custom JavaScript to a user. When the user clicks this phishing link, the browser renders the response of `GET /proxy/<host>`, which runs the custom JavaScript contained in `host` set by the actor. As any arbitrary JavaScript can be run after the user clicks on a phishing link, this issue permits extensive access to the user's JupyterLab instance for an actor. Patches are included in versions 4.2.0 and 3.2.4. As a workaround, server operators who are unable to upgrade can disable the `jupyter-server-proxy` extension.	9.6	More Details
CVE-2024-3166	A Cross-Site Scripting (XSS) vulnerability exists in mintplex-labs/anything-llm, affecting both the desktop application version 1.2.0 and the latest version of the web application. The vulnerability arises from the application's feature to fetch and embed content from websites into workspaces, which can be exploited to execute arbitrary JavaScript code. In the desktop application, this flaw can be escalated to Remote Code Execution (RCE) due to insecure application settings, specifically the enabling of 'nodeIntegration' and the disabling of 'contextIsolation' in Electron's webPreferences. The issue has been addressed in version 1.4.2 of the desktop application.	9.6	More Details
CVE-2024-3033	An improper authorization vulnerability exists in the mintplex-labs/anything-llm application, specifically within the '/api/v/' endpoint and its sub-routes. This flaw allows unauthenticated users to perform destructive actions on the VectorDB, including resetting the database and deleting specific namespaces, without requiring any authorization or permissions. The issue affects all versions up to and including the latest version, with a fix introduced in version 1.0.0. Exploitation of this vulnerability can lead to complete data loss of document embeddings across all workspaces, rendering workspace chats and embeddable chat widgets non-functional. Additionally, attackers can list all namespaces, potentially exposing private workspace names.	9.4	More Details
CVE-2024-36266	A vulnerability has been identified in PowerSys (All versions < V3.11). The affected application insufficiently protects responses to authentication requests. This could allow a local attacker to bypass authentication, thereby gaining administrative privileges for the managed remote devices.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5328	A Server-Side Request Forgery (SSRF) vulnerability exists in the lunary-ai/lunary application, specifically within the endpoint '/auth/saml/tto/download-idp-xml'. The vulnerability arises due to the application's failure to validate user-supplied URLs before using them in server-side requests. An attacker can exploit this vulnerability by sending a specially crafted request to the affected endpoint, allowing them to make unauthorized requests to internal or external resources. This could lead to the disclosure of sensitive information, service disruption, or further attacks against the network infrastructure. The issue affects the latest version of the application as of the report.	9.3	More Details
CVE-2024-37051	GitHub access token could be exposed to third-party sites in JetBrains IDEs after version 2023.1 and less than: IntelliJ IDEA 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; Aqua 2024.1.2; CLion 2023.1.7, 2023.2.4, 2023.3.5, 2024.1.3, 2024.2 EAP2; DataGrip 2023.1.3, 2023.2.4, 2023.3.5, 2024.1.4; DataSpell 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.2, 2024.2 EAP1; GoLand 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP3; MPS 2023.2.1, 2023.3.1, 2024.1 EAP2; PhpStorm 2023.1.6, 2023.2.6, 2023.3.7, 2024.1.3, 2024.2 EAP3; PyCharm 2023.1.6, 2023.2.7, 2023.3.6, 2024.1.3, 2024.2 EAP2; Rider 2023.1.7, 2023.2.5, 2023.3.6, 2024.1.3; RubyMine 2023.1.7, 2023.2.7, 2023.3.7, 2024.1.3, 2024.2 EAP4; RustRover 2024.1.1; WebStorm 2023.1.6, 2023.2.7, 2023.3.7, 2024.1.4	9.3	More Details
CVE-2024-4009	Replay Attack in ABB, Busch-Jaeger, FTS Display (version 1.00) and BCU (version 1.3.0.33) allows attacker to capture/replay KNX telegram to local KNX Bus-System	9.2	More Details
CVE-2024-32167	Sourcecodester Online Medicine Ordering System 1.0 is vulnerable to Arbitrary file deletion vulnerability as the backend settings have the function of deleting pictures to delete any files.	9.1	More Details
CVE-2024-1873	parisneo/lollms-webui is vulnerable to path traversal and denial of service attacks due to an exposed `/select_database` endpoint in version a9d16b0. The endpoint improperly handles file paths, allowing attackers to specify absolute paths when interacting with the `DiscussionsDB` instance. This flaw enables attackers to create directories anywhere on the system where the application has permissions, potentially leading to denial of service by creating directories with names of critical files, such as HTTPS certificate files, causing server startup failures. Additionally, attackers can manipulate the database path, resulting in the loss of client data by constantly changing the file location to an attacker-controlled location, scattering the data across the filesystem and making recovery difficult.	9.1	More Details
CVE-2024-32752	Under certain circumstances communications between the ICU tool and an iSTAR Pro door controller is susceptible to Machine-in-the-Middle attacks which could impact door control and configuration.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34405	Improper deep link validation in McAfee Security: Antivirus VPN for Android before 8.3.0 could allow an attacker to launch an arbitrary URL within the app.	9.1	More Details
CVE-2024-24192	robdns commit d76d2e6 was discovered to contain a heap overflow via the component block->filename at /src/zonefile-insertion.c.	9.1	More Details
CVE-2024-2012	vulnerability exists in the FOXMAN-UN/UNEM server / API Gateway that if exploited an attacker could use to allow unintended commands or code to be executed on the UNEM server allowing sensitive data to be read or modified or could cause other unintended behavior	9.1	More Details
CVE-2024-2362	A path traversal vulnerability exists in the parisneo/lollms-webui version 9.3 on the Windows platform. Due to improper validation of file paths between Windows and Linux environments, an attacker can exploit this vulnerability to delete any file on the system. The issue arises from the lack of adequate sanitization of user-supplied input in the 'del_preset' endpoint, where the application fails to prevent the use of absolute paths or directory traversal sequences ('..'). As a result, an attacker can send a specially crafted request to the 'del_preset' endpoint to delete files outside of the intended directory.	9.1	More Details
CVE-2024-5153	The Startklar Elementor Addons plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.7.15 via the 'dropzone_hash' parameter. This makes it possible for unauthenticated attackers to copy the contents of arbitrary files on the server, which can contain sensitive information, and to delete arbitrary directories, including the root WordPress directory.	9.1	More Details
CVE-2024-31611	SeaCMS 12.9 has a file deletion vulnerability via admin_template.php.	9.1	More Details
CVE-2024-37388	An XML External Entity (XXE) vulnerability in the ebookmeta.get_metadata function of lxml before v4.9.1 allows attackers to access sensitive information or cause a Denial of Service (DoS) via crafted XML input.	9.1	More Details
CVE-2024-37407	Libarchive before 3.7.4 allows name out-of-bounds access when a ZIP archive has an empty-name file and mac-ext is enabled. This occurs in slurp_central_directory in archive_read_support_format_zip.c.	9.1	More Details
CVE-2024-36415	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in uploaded file verification in products allows for remote code execution. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33565	Missing Authorization vulnerability in UkrSolution Barcode Scanner with Inventory & Order Manager.This issue affects Barcode Scanner with Inventory & Order Manager: from n/a through 1.5.3.	9.1	More Details
CVE-2024-36394	SysAid - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	9.1	More Details
CVE-2024-35677	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in StylemixThemes MegaMenu allows PHP Local File Inclusion.This issue affects MegaMenu: from n/a through 2.3.12.	9.0	More Details
CVE-2024-31401	Cross-site scripting vulnerability in Cybozu Garoon 5.0.0 to 5.15.2 allows a remote authenticated attacker with an administrative privilege to inject an arbitrary script on the web browser of the user who is logging in to the product.	9.0	More Details
CVE-2024-35213	An improper input validation vulnerability in the SGI Image Codec of QNX SDP version(s) 6.6, 7.0, and 7.1 could allow an attacker to potentially cause a denial-of-service condition or execute code in the context of the image processing process.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-36413	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in the import module error view allows for a cross-site scripting attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	8.9	More Details
CVE-2024-37166	ghtml is software that uses tagged templates for template engine functionality. It is possible to introduce user-controlled JavaScript code and trigger a Cross-Site Scripting (XSS) vulnerability in some cases. Version 2.0.0 introduces changes to mitigate this issue. Version 2.0.0 contains updated documentation to clarify that while ghtml escapes characters with special meaning in HTML, it does not provide comprehensive protection against all types of XSS attacks in every scenario. This aligns with the approach taken by other template engines. Developers should be cautious and take additional measures to sanitize user input and prevent potential vulnerabilities. Additionally, the backtick character (`) is now also escaped to prevent the creation of strings in most cases where a malicious actor somehow gains the ability to write JavaScript. This does not provide comprehensive protection either.	8.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5847	Use after free in PDFium in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-33564	Missing Authorization vulnerability in 8theme XStore.This issue affects XStore: from n/a through 9.3.8.	8.8	More Details
CVE-2024-36668	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component admin/type_deal.php?mudi=del	8.8	More Details
CVE-2024-36667	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/idcProType_deal.php?mudi=add&nohrefStr=close	8.8	More Details
CVE-2024-5267	Sonos Era 100 SMB2 Message Handling Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Sonos Era 100 smart speakers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of SMB2 messages. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-22384.	8.8	More Details
CVE-2024-5269	Sonos Era 100 SMB2 Message Handling Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Sonos Era 100 smart speakers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of SMB2 messages. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-22459.	8.8	More Details
CVE-2024-5505	NETGEAR ProSAFE Network Management System UpLoadServlet Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Authentication is required to exploit this vulnerability. The specific flaw exists within the UpLoadServlet class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-22724.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0520	A vulnerability in mlflow/mlflow version 8.2.1 allows for remote code execution due to improper neutralization of special elements used in an OS command ('Command Injection') within the `mlflow.data.http_dataset_source.py` module. Specifically, when loading a dataset from a source URL with an HTTP scheme, the filename extracted from the `Content-Disposition` header or the URL path is used to generate the final file path without proper sanitization. This flaw enables an attacker to control the file path fully by utilizing path traversal or absolute path techniques, such as '../../tmp/poc.txt' or '/tmp/poc.txt', leading to arbitrary file write. Exploiting this vulnerability could allow a malicious user to execute commands on the vulnerable machine, potentially gaining access to data and model information. The issue is fixed in version 2.9.0.	8.8	More Details
CVE-2024-30485	Missing Authorization vulnerability in XLPlugins Finale Lite.This issue affects Finale Lite: from n/a through 2.18.0.	8.8	More Details
CVE-2024-36670	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component admin/vpsClass_deal.php?mudi=del	8.8	More Details
CVE-2024-25092	Missing Authorization vulnerability in XLPlugins NextMove Lite.This issue affects NextMove Lite: from n/a through 2.17.0.	8.8	More Details
CVE-2024-30064	Windows Kernel Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-30068	Windows Kernel Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-4680	A vulnerability in zenml-io/zenml version 0.56.3 allows attackers to reuse old session credentials or session IDs due to insufficient session expiration. Specifically, the session does not expire after a password change, enabling an attacker to maintain access to a compromised account without the victim's ability to revoke this access. This issue was observed in a self-hosted ZenML deployment via Docker, where after changing the password from one browser, the session remained active and usable in another browser without requiring re-authentication.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3668	The PowerPack Pro for Elementor plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 2.10.17. This is due to the plugin not restricting low privileged users from setting a default role for a registration form. This makes it possible for authenticated attackers, with contributor-level access and above, to create a registration form with administrator set as the default role and then register as an administrator.	8.8	More Details
CVE-2024-30078	Windows Wi-Fi Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-36669	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component admin/type_deal.php?mudi=add.	8.8	More Details
CVE-2024-37569	An issue was discovered on Mitel 6869i through 4.5.0.41 and 5.x through 5.0.0.1018 devices. A command injection vulnerability exists in the hostname parameter taken in by the provis.html endpoint. The provis.html endpoint performs no sanitization on the hostname parameter (sent by an authenticated user), which is subsequently written to disk. During boot, the hostname parameter is executed as part of a series of shell commands. Attackers can achieve remote code execution in the root context by placing shell metacharacters in the hostname parameter.	8.8	More Details
CVE-2024-3149	A Server-Side Request Forgery (SSRF) vulnerability exists in the upload link feature of mintplex-labs/anything-llm. This feature, intended for users with manager or admin roles, processes uploaded links through an internal Collector API using a headless browser. An attacker can exploit this by hosting a malicious website and using it to perform actions such as internal port scanning, accessing internal web applications not exposed externally, and interacting with the Collector API. This interaction can lead to unauthorized actions such as arbitrary file deletion and limited Local File Inclusion (LFI), including accessing NGINX access logs which may contain sensitive information.	8.8	More Details
CVE-2024-5179	The Cowidgets – Elementor Addons plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.1.1 via the 'item_style' and 'style' parameters. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27820	The issue was addressed with improved memory handling. This issue is fixed in tvOS 17.5, iOS 16.7.8 and iPadOS 16.7.8, visionOS 1.2, Safari 17.5, iOS 17.5 and iPadOS 17.5, watchOS 10.5, macOS Sonoma 14.5. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2024-5329	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to blind SQL Injection via the ‘data[addonID]’ parameter in all versions up to, and including, 1.5.109 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.	8.8	More Details
CVE-2024-27833	An integer overflow was addressed with improved input validation. This issue is fixed in tvOS 17.5, iOS 16.7.8 and iPadOS 16.7.8, visionOS 1.2, Safari 17.5, iOS 17.5 and iPadOS 17.5. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2024-27851	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 17.5, visionOS 1.2, Safari 17.5, iOS 17.5 and iPadOS 17.5, watchOS 10.5, macOS Sonoma 14.5. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2024-5324	The Login/Signup Popup (Inline Form + Woocommerce) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'import_settings' function in versions 2.7.1 to 2.7.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change arbitrary options on affected sites. This can be used to enable new user registration and set the default role for new users to Administrator.	8.8	More Details
CVE-2024-27855	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.5, macOS Ventura 13.6.7, iOS 17.5 and iPadOS 17.5, iOS 16.7.8 and iPadOS 16.7.8. A shortcut may be able to use sensitive data with certain actions without prompting the user.	8.8	More Details
CVE-2024-36528	nukeviet v.4.5 and before and nukeviet-egov v.1.2.02 and before have a Deserialization vulnerability which results in code execution via /admin/extensions/download.php and /admin/extensions/upload.php.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3152	mintplex-labs/anything-llm is vulnerable to multiple security issues due to improper input validation in several endpoints. An attacker can exploit these vulnerabilities to escalate privileges from a default user role to an admin role, read and delete arbitrary files on the system, and perform Server-Side Request Forgery (SSRF) attacks. The vulnerabilities are present in the `/request-token`, `/workspace/:slug/thread/:threadSlug/update`, `/system/remove-logo`, `/system/logo`, and collector's `/process` endpoints. These issues are due to the application's failure to properly validate user input before passing it to `prisma` functions and other critical operations. Affected versions include the latest version prior to 1.0.0.	8.8	More Details
CVE-2024-35241	Composer is a dependency manager for PHP. On the 2.x branch prior to versions 2.2.24 and 2.7.7, the `status`, `reinstall` and `remove` commands with packages installed from source via git containing specially crafted branch names in the repository can be used to execute code. Patches for this issue are available in version 2.2.24 for 2.2 LTS or 2.7.7 for mainline. As a workaround, avoid installing dependencies via git by using `--prefer-dist` or the `preferred-install: dist` config setting.	8.8	More Details
CVE-2024-35242	Composer is a dependency manager for PHP. On the 2.x branch prior to versions 2.2.24 and 2.7.7, the `composer install` command running inside a git/hg repository which has specially crafted branch names can lead to command injection. This requires cloning untrusted repositories. Patches are available in version 2.2.24 for 2.2 LTS or 2.7.7 for mainline. As a workaround, avoid cloning potentially compromised repositories.	8.8	More Details
CVE-2024-1879	A Cross-Site Request Forgery (CSRF) vulnerability in significant-gravitas/autogpt version v0.5.0 allows attackers to execute arbitrary commands on the AutoGPT server. The vulnerability stems from the lack of protections on the API endpoint receiving instructions, enabling an attacker to direct a user running AutoGPT in their local network to a malicious website. This site can then send crafted requests to the AutoGPT server, leading to command execution. The issue is exacerbated by CORS being enabled for arbitrary origins by default, allowing the attacker to read the response of all cross-site queries. This vulnerability was addressed in version 5.1.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2914	A TarSlip vulnerability exists in the deepjavalibrary/djl, affecting version 0.26.0 and fixed in version 0.27.0. This vulnerability allows an attacker to manipulate file paths within tar archives to overwrite arbitrary files on the target system. Exploitation of this vulnerability could lead to remote code execution, privilege escalation, data theft or manipulation, and denial of service. The vulnerability is due to improper validation of file paths during the extraction of tar files, as demonstrated in multiple occurrences within the library's codebase, including but not limited to the files_util.py and extract_imagenet.py scripts.	8.8	More Details
CVE-2024-30368	A10 Thunder ADC CsrRequestView Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of A10 Thunder ADC. Authentication is required to exploit this vulnerability. The specific flaw exists within the CsrRequestView class. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of a10user. Was ZDI-CAN-22517.	8.8	More Details
CVE-2024-37570	On Mitel 6869i 4.5.0.41 devices, the Manual Firmware Update (upgrade.html) page does not perform sanitization on the username and path parameters (sent by an authenticated user) before appending flags to the busybox ftpget command. This leads to $() command execution.	8.8	More Details
CVE-2024-0444	GStreamer AV1 Video Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GStreamer. Interaction with this library is required to exploit this vulnerability but attack vectors may vary depending on the implementation. The specific flaw exists within the parsing of tile list data within AV1-encoded video files. 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 current process. Was ZDI-CAN-22873.	8.8	More Details
CVE-2024-27808	The issue was addressed with improved memory handling. This issue is fixed in tvOS 17.5, visionOS 1.2, Safari 17.5, iOS 17.5 and iPadOS 17.5, watchOS 10.5, macOS Sonoma 14.5. Processing web content may lead to arbitrary code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3150	In mintplex-labs/anything-llm, a vulnerability exists in the thread update process that allows users with Default or Manager roles to escalate their privileges to Administrator. The issue arises from improper input validation when handling HTTP POST requests to the endpoint `/workspace/:slug/thread/:threadSlug/update`. Specifically, the application fails to validate or check user input before passing it to the `workspace_thread` Prisma model for execution. This oversight allows attackers to craft a Prisma relation query operation that manipulates the `users` model to change a user's role to admin. Successful exploitation grants attackers the highest level of user privileges, enabling them to see and perform all actions within the system.	8.8	More Details
CVE-2024-5128	An Insecure Direct Object Reference (IDOR) vulnerability was identified in lunary-ai/lunary, affecting versions up to and including 1.2.2. This vulnerability allows unauthorized users to view, update, or delete any dataset_prompt or dataset_prompt_variation within any dataset or project. The issue stems from improper access control checks in the dataset management endpoints, where direct references to object IDs are not adequately secured against unauthorized access. This vulnerability was fixed in version 1.2.25.	8.8	More Details
CVE-2024-36790	Netgear WNR614 JNR1010V2/N300-V1.1.0.54_1.0.1 was discovered to store credentials in plaintext.	8.8	More Details
CVE-2024-35249	Microsoft Dynamics 365 Business Central Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-5187	A vulnerability in the `download_model_with_test_data` function of the onnx/onnx framework, version 1.16.0, allows for arbitrary file overwrite due to inadequate prevention of path traversal attacks in malicious tar files. This vulnerability enables attackers to overwrite any file on the system, potentially leading to remote code execution, deletion of system, personal, or application files, thus impacting the integrity and availability of the system. The issue arises from the function's handling of tar file extraction without performing security checks on the paths within the tar file, as demonstrated by the ability to overwrite the `/home/kali/.ssh/authorized_keys` file by specifying an absolute path in the malicious tar file.	8.8	More Details
CVE-2024-36787	An issue in Netgear WNR614 JNR1010V2 N300-V1.1.0.54_1.0.1 allows attackers to bypass authentication and access the administrative interface via unspecified vectors.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28877	MicroDicom DICOM Viewer is vulnerable to a stack-based buffer overflow, which may allow an attacker to execute arbitrary code on affected installations of DICOM Viewer. User interaction is required to exploit this vulnerability.	8.8	More Details
CVE-2024-30103	Microsoft Outlook Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-33606	An attacker could retrieve sensitive files (medical images) as well as plant new medical images or overwrite existing medical images on a MicroDicom DICOM Viewer system. User interaction is required to exploit this vulnerability.	8.8	More Details
CVE-2024-5830	Type Confusion in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5831	Use after free in Dawn in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5832	Use after free in Dawn in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5833	Type Confusion in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5834	Inappropriate implementation in Dawn in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5835	Heap buffer overflow in Tab Groups in Google Chrome prior to 126.0.6478.54 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5836	Inappropriate Implementation in DevTools in Google Chrome prior to 126.0.6478.54 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. (Chromium security severity: High)	8.8	More Details
CVE-2024-5837	Type Confusion in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5838	Type Confusion in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5841	Use after free in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-5842	Use after free in Browser UI in Google Chrome prior to 126.0.6478.54 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-30097	Microsoft Speech Application Programming Interface (SAPI) Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-5844	Heap buffer overflow in Tab Strip in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-5845	Use after free in Audio in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-5846	Use after free in PDFium in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-49222	Precor touchscreen console P82 contains a private SSH key that corresponds to a default public key. A remote attacker could exploit this to gain root privileges.	8.8	More Details
CVE-2023-49223	Precor touchscreen console P62, P80, and P82 could allow a remote attacker to obtain sensitive information because the root password is stored in /etc/passwd. An attacker could exploit this to extract files and obtain sensitive information.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3110	A stored Cross-Site Scripting (XSS) vulnerability exists in the mintplex-labs/anything-llm application, affecting versions up to and including the latest before 1.0.0. The vulnerability arises from the application's failure to properly sanitize and validate user-supplied URLs before embedding them into the application UI as external links with custom icons. Specifically, the application does not prevent the inclusion of 'javascript:' protocol payloads in URLs, which can be exploited by a user with manager role to execute arbitrary JavaScript code in the context of another user's session. This flaw can be leveraged to steal the admin's authorization token by crafting malicious URLs that, when clicked by the admin, send the token to an attacker-controlled server. The attacker can then use this token to perform unauthorized actions, escalate privileges to admin, or directly take over the admin account. The vulnerability is triggered when the malicious link is opened in a new tab using either the CTRL + left mouse button click or the mouse scroll wheel click, or in some non-updated versions of modern browsers, by directly clicking on the link.	8.7	More Details
CVE-2024-35658	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ThemeHigh Checkout Field Editor for WooCommerce (Pro) allows Functionality Misuse, File Manipulation.This issue affects Checkout Field Editor for WooCommerce (Pro): from n/a through 3.6.2.	8.6	More Details
CVE-2024-35743	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Siteclean SC filechecker allows Path Traversal, File Manipulation.This issue affects SC filechecker: from n/a through 0.6.	8.6	More Details
CVE-2024-35744	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ravidhu Dissanayake Upunzipper allows Path Traversal, File Manipulation.This issue affects Upunzipper: from n/a through 1.0.0.	8.6	More Details
CVE-2024-28995	SolarWinds Serv-U was susceptible to a directory transversal vulnerability that would allow access to read sensitive files on the host machine.	8.6	More Details
CVE-2024-23299	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Ventura 13.6.5, macOS Monterey 12.7.4. An app may be able to break out of its sandbox.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5186	A Server-Side Request Forgery (SSRF) vulnerability exists in the file upload section of imartinez/privategpt version 0.5.0. This vulnerability allows attackers to send crafted requests that could result in unauthorized access to the local network and potentially sensitive information. Specifically, by manipulating the 'path' parameter in a file upload request, an attacker can cause the application to make arbitrary requests to internal services, including the AWS metadata endpoint. This issue could lead to the exposure of internal servers and sensitive data.	8.6	More Details
CVE-2024-4325	A Server-Side Request Forgery (SSRF) vulnerability exists in the gradio-app/gradio version 4.21.0, specifically within the `/queue/join` endpoint and the `save_url_to_cache` function. The vulnerability arises when the `path` value, obtained from the user and expected to be a URL, is used to make an HTTP request without sufficient validation checks. This flaw allows an attacker to send crafted requests that could lead to unauthorized access to the local network or the AWS metadata endpoint, thereby compromising the security of internal servers.	8.6	More Details
CVE-2024-2011	A heap-based buffer overflow vulnerability exists in the FOXMAN-UN/UNEM that if exploited will generally lead to a denial of service but can be used to execute arbitrary code, which is usually outside the scope of a program's implicit security policy	8.6	More Details
CVE-2024-36416	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a deprecated v4 API example with no log rotation allows denial of service by logging excessive data. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	8.6	More Details
CVE-2024-5696	By manipulating the text in an `&lt;input&gt;` tag, an attacker could have caused corrupt memory leading to a potentially exploitable crash. This vulnerability affects Firefox < 127, Firefox ESR < 115.12, and Thunderbird < 115.12.	8.6	More Details
CVE-2023-52233	Missing Authorization vulnerability in Post SMTP Post SMTP Mailer/Email Log.This issue affects Post SMTP Mailer/Email Log: from n/a through 2.8.6.	8.6	More Details
CVE-2024-24703	Missing Authorization vulnerability in MultiVendorX WC Marketplace.This issue affects WC Marketplace: from n/a through 4.0.25.	8.6	More Details
CVE-2024-32778	Missing Authorization vulnerability in Contest Gallery.This issue affects Contest Gallery: from n/a through 21.3.4.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34761	Vulnerability discovered by executing a planned security audit. Improper Control of Generation of Code ('Code Injection') vulnerability in WPENGINE INC Advanced Custom Fields PRO allows Code Injection.This issue affects Advanced Custom Fields PRO: from n/a before 6.2.10.	8.5	More Details
CVE-2024-36418	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in connectors allows an authenticated user to perform a remote code execution attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	8.5	More Details
CVE-2024-35678	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BestWebSoft Contact Form to DB by BestWebSoft.This issue affects Contact Form to DB by BestWebSoft: from n/a through 1.7.2.	8.5	More Details
CVE-2024-35750	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in wpdevart Responsive Image Gallery, Gallery Album.This issue affects Responsive Image Gallery, Gallery Album: from n/a through 2.0.3.	8.5	More Details
CVE-2024-35736	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeisle Visualizer.This issue affects Visualizer: from n/a through 3.11.1.	8.5	More Details
CVE-2024-32502	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 reference count checking, which can result in a UAF (Use-After-Free) vulnerability.	8.4	More Details
CVE-2023-37539	The Domino Catalog template is susceptible to a Stored Cross-Site Scripting (XSS) vulnerability. An attacker with the ability to edit documents in the catalog application/database created from this template can embed a cross site scripting attack. The attack would be activated by an end user clicking it.	8.4	More Details
CVE-2024-32503	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 memory deallocation checking, which can result in a UAF (Use-After-Free) vulnerability.	8.4	More Details
CVE-2024-31959	An issue was discovered in Samsung Mobile Processor Exynos 2200, Exynos 1480, Exynos 2400. It lacks a check for the validation of native handles, which can result in code execution.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31080	Missing Authorization vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates).This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 1.5.65.	8.3	More Details
CVE-2024-2288	A Cross-Site Request Forgery (CSRF) vulnerability exists in the profile picture upload functionality of the Lollms application, specifically in the parisneo/lollms-webui repository, affecting versions up to 7.3.0. This vulnerability allows attackers to change a victim's profile picture without their consent, potentially leading to a denial of service by overloading the filesystem with files. Additionally, this flaw can be exploited to perform a stored cross-site scripting (XSS) attack, enabling attackers to execute arbitrary JavaScript in the context of the victim's browser session. The issue is resolved in version 9.3.	8.3	More Details
CVE-2023-25799	Missing Authorization vulnerability in Themeum Tutor LMS.This issue affects Tutor LMS: from n/a through 2.1.8.	8.3	More Details
CVE-2024-33547	Missing Authorization vulnerability in AA-Team WZone.This issue affects WZone: from n/a through 14.0.10.	8.3	More Details
CVE-2024-36129	The OpenTelemetry Collector offers a vendor-agnostic implementation on how to receive, process and export telemetry data. An unsafe decompression vulnerability allows unauthenticated attackers to crash the collector via excessive memory consumption. OTel Collector version 0.102.1 fixes this issue. It is also fixed in the confighttp module version 0.102.0 and configgrpc module version 0.102.1.	8.2	More Details
CVE-2024-36399	Kanboard is project management software that focuses on the Kanban methodology. The vuln is in app/Controller/ProjectPermissionController.php function addUser(). The users permission to add users to a project only get checked on the URL parameter project_id. If the user is authorized to add users to this project the request gets processed. The users permission for the POST BODY parameter project_id does not get checked again while processing. An attacker with the 'Project Manager' on a single project may take over any other project. The vulnerability is fixed in 1.2.37.	8.2	More Details
CVE-2024-5129	A Privilege Escalation Vulnerability exists in lunary-ai/lunary version 1.2.2, where any user can delete any datasets due to missing authorization checks. The vulnerability is present in the dataset deletion functionality, where the application fails to verify if the user requesting the deletion has the appropriate permissions. This allows unauthorized users to send a DELETE request to the server and delete any dataset by specifying its ID. The issue is located in the datasets.delete function within the datasets index file.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35292	A vulnerability has been identified in SIMATIC S7-200 SMART CPU CR40 (6ES7288-1CR40-0AA0) (All versions), SIMATIC S7-200 SMART CPU CR60 (6ES7288-1CR60-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA1) (All versions), SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA0) (All versions), SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA1) (All versions), SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA0) (All versions), SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA1) (All versions). Affected devices are using a predictable IP ID sequence number. This leaves the system susceptible to a family of attacks which rely on the use of predictable IP ID sequence numbers as their base method of attack and eventually could allow an attacker to create a denial of service condition.	8.2	More Details
CVE-2023-45192	IBM Engineering Requirements Management DOORS Next 7.0.2 and 7.0.3 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 268758.	8.2	More Details
CVE-2024-36792	An issue in the implementation of the WPS in Netgear WNR614 JNR1010V2/N300-V1.1.0.54_1.0.1 allows attackers to gain access to the router's pin.	8.2	More Details
CVE-2024-31275	Missing Authorization vulnerability in Metagauss EventPrime.This issue affects EventPrime: from n/a through 3.3.4.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5133	In lunary-ai/lunary version 1.2.4, an account takeover vulnerability exists due to the exposure of password recovery tokens in API responses. Specifically, when a user initiates the password reset process, the recovery token is included in the response of the `GET /v1/users/me/org` endpoint, which lists all users in a team. This allows any authenticated user to capture the recovery token of another user and subsequently change that user's password without consent, effectively taking over the account. The issue lies in the inclusion of the `recovery_token` attribute in the users object returned by the API.	8.1	More Details
CVE-2024-4328	A Cross-Site Request Forgery (CSRF) vulnerability exists in the clear_personality_files_list function of the parisneo/lollms-webui v9.6. The vulnerability arises from the use of a GET request to clear personality files list, which lacks proper CSRF protection. This flaw allows attackers to trick users into performing actions without their consent, such as deleting important files on the system. The issue is present in the application's handling of requests, making it susceptible to CSRF attacks that could lead to unauthorized actions being performed on behalf of the user.	8.1	More Details
CVE-2024-33555	Missing Authorization vulnerability in 8theme XStore Core.This issue affects XStore Core: from n/a through 5.3.8.	8.1	More Details
CVE-2024-31098	Missing Authorization vulnerability in Mr.Ebabi New Order Notification for Woocommerce.This issue affects New Order Notification for Woocommerce: from n/a through 2.0.2.	8.1	More Details
CVE-2024-5389	In lunary-ai/lunary version 1.2.13, an insufficient granularity of access control vulnerability allows users to create, update, get, and delete prompt variations for datasets not owned by their organization. This issue arises due to the application not properly validating the ownership of dataset prompts and their variations against the organization or project of the requesting user. As a result, unauthorized modifications to dataset prompts can occur, leading to altered or removed dataset prompts without proper authorization. This vulnerability impacts the integrity and consistency of dataset information, potentially affecting the results of experiments.	8.1	More Details
CVE-2024-4888	BerriAI's litellm, in its latest version, is vulnerable to arbitrary file deletion due to improper input validation on the `/audio/transcriptions` endpoint. An attacker can exploit this vulnerability by sending a specially crafted request that includes a file path to the server, which then deletes the specified file without proper authorization or validation. This vulnerability is present in the code where `os.remove(file.filename)` is used to delete a file, allowing any user to delete critical files on the server such as SSH keys, SQLite databases, or configuration files.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36789	An issue in Netgear WNR614 JNR1010V2/N300-V1.1.0.54_1.0.1 allows attackers to create passwords that do not conform to defined security standards.	8.1	More Details
CVE-2024-4177	A host whitelist parser issue in the proxy service implemented in the GravityZone Update Server allows an attacker to cause a server-side request forgery. This issue only affects GravityZone Console versions before 6.38.1-2 that are running only on premise.	8.1	More Details
CVE-2024-37177	SAP Financial Consolidation allows data to enter a Web application through an untrusted source. These endpoints are exposed over the network and it allows the user to modify the content from the web site. On successful exploitation, an attacker can cause significant impact to confidentiality and integrity of the application.	8.1	More Details
CVE-2023-6966	The The Moneytizer plugin for WordPress is vulnerable to unauthorized access of data, modification of data, and loss of data due to a missing capability check on multiple AJAX functions in the /core/core_ajax.php file in all versions up to, and including, 9.5.20. This makes it possible for authenticated attackers, with subscriber access and above, to update and retrieve billing and bank details, update and reset the plugin's settings, and update languages as well as other lower-severity actions.	8.1	More Details
CVE-2024-37325	Azure Science Virtual Machine (DSVM) Elevation of Privilege Vulnerability	8.1	More Details
CVE-2024-5688	If a garbage collection was triggered at the right time, a use-after-free could have occurred during object transplant. This vulnerability affects Firefox < 127, Firefox ESR < 115.12, and Thunderbird < 115.12.	8.1	More Details
CVE-2023-6968	The The Moneytizer plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 9.5.20. This is due to missing or incorrect nonce validation on multiple AJAX functions. This makes it possible for unauthenticated attackers to to update and retrieve billing and bank details, update and reset the plugin's settings, and update languages as well as other lower-severity actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.1	More Details
CVE-2024-4190	Stored Cross-Site Scripting (XSS) vulnerabilities have been identified in OpenText ArcSight Logger. The vulnerabilities could be remotely exploited.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7264	The Build App Online plugin for WordPress is vulnerable to account takeover due to a weak password reset mechanism in all versions up to, and including, 1.0.21. This makes it possible for unauthenticated attackers to reset the password of arbitrary users by guessing an 4-digit numeric reset code.	8.1	More Details
CVE-2024-30075	Windows Link Layer Topology Discovery Protocol Remote Code Execution Vulnerability	8.0	More Details
CVE-2023-49224	Precor touchscreen console P62, P80, and P82 contains a default SSH public key in the authorized_keys file. A remote attacker could use this key to gain root privileges.	8.0	More Details
CVE-2024-28020	A user/password reuse vulnerability exists in the FOXMAN-UN/UNEM application and server management. If exploited a malicious high-privileged user could use the passwords and login information through complex routines to extend access on the server and other services.	8.0	More Details
CVE-2024-5785	Command injection vulnerability in Comtrend router WLD71-T1_v2.0.201820, affecting the GRG-4280us version. This vulnerability could allow an authenticated user to execute commands inside the router by making a POST request to the URL “/boaform/admin/formUserTracert”.	8.0	More Details
CVE-2024-30077	Windows OLE Remote Code Execution Vulnerability	8.0	More Details
CVE-2024-30074	Windows Link Layer Topology Discovery Protocol Remote Code Execution Vulnerability	8.0	More Details
CVE-2024-5303	Kofax Power PDF PSD File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Kofax Power PDF. 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 parsing of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-22919.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5301	Kofax Power PDF PSD File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Kofax Power PDF. 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 parsing of PSD files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-22917.	7.8	More Details
CVE-2024-35303	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0012), Tecnomatix Plant Simulation V2404 (All versions < V2404.0001). The affected applications contain a type confusion vulnerability while parsing specially crafted MODEL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-22958)	7.8	More Details
CVE-2024-5302	Kofax Power PDF PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Kofax Power PDF. 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 parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-22918.	7.8	More Details
CVE-2024-35206	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected application does not expire the session. This could allow an attacker to get unauthorized access.	7.8	More Details
CVE-2024-4610	Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver allows a local non-privileged user to make improper GPU memory processing operations to gain access to already freed memory.This issue affects Bifrost GPU Kernel Driver: from r34p0 through r40p0; Valhall GPU Kernel Driver: from r34p0 through r40p0.	7.8	More Details
CVE-2024-5506	Luxion KeyShot Viewer KSP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Luxion KeyShot Viewer. 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 parsing of KSP files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-22514.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1880	An OS command injection vulnerability exists in the MacOS Text-To-Speech class MacOSTTS of the significant-gravitas/autogpt project, affecting versions up to v0.5.0. The vulnerability arises from the improper neutralization of special elements used in an OS command within the `_speech` method of the MacOSTTS class. Specifically, the use of `os.system` to execute the `say` command with user-supplied text allows for arbitrary code execution if an attacker can inject shell commands. This issue is triggered when the AutoGPT instance is run with the `--speak` option enabled and configured with `TEXT_TO_SPEECH_PROVIDER=macos`, reflecting back a shell injection snippet. The impact of this vulnerability is the potential execution of arbitrary code on the instance running AutoGPT. The issue was addressed in version 5.1.0.	7.8	More Details
CVE-2024-5509	Luxion KeyShot BIP File Parsing Uncontrolled Search Path Element Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Luxion KeyShot. 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 parsing of BIP files. The issue results from loading a library from an unsecured location. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-22738.	7.8	More Details
CVE-2024-5508	Luxion KeyShot Viewer KSP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Luxion KeyShot Viewer. 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 parsing of KSP files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-22267.	7.8	More Details
CVE-2024-5507	Luxion KeyShot Viewer KSP File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Luxion KeyShot Viewer. 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 parsing of KSP files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-22266.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35207	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The web interface of the affected devices are vulnerable to Cross-Site Request Forgery(CSRF) attacks. By tricking an authenticated victim user to click a malicious link, an attacker could perform arbitrary actions on the device on behalf of the victim user.	7.8	More Details
CVE-2024-27801	The issue was addressed with improved checks. This issue is fixed in tvOS 17.5, visionOS 1.2, iOS 17.5 and iPadOS 17.5, watchOS 10.5, macOS Sonoma 14.5. An app may be able to elevate privileges.	7.8	More Details
CVE-2024-5305	Kofax Power PDF PDF File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Kofax Power PDF. 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 parsing of PDF files. 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 current process. Was ZDI-CAN-22921.	7.8	More Details
CVE-2024-30373	Kofax Power PDF JPF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Kofax Power PDF. 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 parsing of JPF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-22092.	7.8	More Details
CVE-2024-30094	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-30091	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-30100	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-49221	Precor touchscreen console P62, P80, and P82 could allow a remote attacker (within the local network) to bypass security restrictions, and access the service menu, because there is a hard-coded service code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30089	Microsoft Streaming Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-30087	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-30086	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-30085	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-7261	Inappropriate implementation in Google Updator prior to 1.3.36.351 in Google Chrome allowed a local attacker to perform privilege escalation via a malicious file. (Chromium security severity: High)	7.8	More Details
CVE-2024-1694	Inappropriate implementation in Google Updator prior to 1.3.36.351 in Google Chrome allowed a local attacker to bypass discretionary access control via a malicious file. (Chromium security severity: High)	7.8	More Details
CVE-2024-30082	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-30072	Microsoft Event Trace Log File Parsing Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-30104	Microsoft Office Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-30062	Windows Standards-Based Storage Management Service Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-35250	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-23110	A stack-based buffer overflow in Fortinet FortiOS version 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0 all versions allows attacker to execute unauthorized code or commands via specially crafted commands	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5304	Kofax Power PDF TGA File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Kofax Power PDF. 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 parsing of TGA files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-22920.	7.8	More Details
CVE-2024-30095	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-27832	The issue was addressed with improved checks. This issue is fixed in tvOS 17.5, visionOS 1.2, iOS 17.5 and iPadOS 17.5, watchOS 10.5, macOS Sonoma 14.5. An app may be able to elevate privileges.	7.8	More Details
CVE-2024-27831	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.6.7, macOS Monterey 12.7.5, iOS 16.7.8 and iPadOS 16.7.8, tvOS 17.5, visionOS 1.2, iOS 17.5 and iPadOS 17.5, macOS Sonoma 14.5. Processing a file may lead to unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2024-27848	This issue was addressed with improved permissions checking. This issue is fixed in macOS Sonoma 14.5, iOS 17.5 and iPadOS 17.5. A malicious app may be able to gain root privileges.	7.8	More Details
CVE-2024-34332	An issue in SiSoftware SANDRA v31.66 (SANDRA.sys 15.18.1.1) and before allows an attacker to escalate privileges via a crafted buffer sent to the Kernel Driver using the DeviceIoControl Windows API.	7.8	More Details
CVE-2024-26507	An issue in FinalWire AIRDA Extreme, AIDA64 Engineer, AIDA64 Business, AIDA64 Network Audit v.7.00.6700 and before allows a local attacker to escalate privileges via the DeviceIoControl call associated with MmMapIoSpace, IoAllocateMdl, MmBuildMdlForNonPagedPool, or MmMapLockedPages components.	7.8	More Details
CVE-2024-27828	The issue was addressed with improved memory handling. This issue is fixed in visionOS 1.2, watchOS 10.5, tvOS 17.5, iOS 17.5 and iPadOS 17.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5306	Kofax Power PDF PDF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Kofax Power PDF. 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 parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-22930.	7.8	More Details
CVE-2024-27857	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in visionOS 1.2, macOS Sonoma 14.5, tvOS 17.5, iOS 17.5 and iPadOS 17.5. A remote attacker may be able to cause unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2024-5597	Fuji Electric Monitouch V-SFT is vulnerable to a type confusion, which could cause a crash or code execution.	7.8	More Details
CVE-2024-32849	Trend Micro Security 17.x (Consumer) is vulnerable to a Privilege Escalation vulnerability that could allow a local attacker to unintentionally delete privileged Trend Micro files including its own.	7.8	More Details
CVE-2024-36971	In the Linux kernel, the following vulnerability has been resolved: net: fix __dst_negative_advice() race __dst_negative_advice() does not enforce proper RCU rules when sk->dst_cache must be cleared, leading to possible UAF. RCU rules are that we must first clear sk->sk_dst_cache, then call dst_release(old_dst). Note that sk_dst_reset(sk) is implementing this protocol correctly, while __dst_negative_advice() uses the wrong order. Given that ip6_negative_advice() has special logic against RTF_CACHE, this means each of the three ->negative_advice() existing methods must perform the sk_dst_reset() themselves. Note the check against NULL dst is centralized in __dst_negative_advice(), there is no need to duplicate it in various callbacks. Many thanks to Clement Lecigne for tracking this issue. This old bug became visible after the blamed commit, using UDP sockets.	7.8	More Details
CVE-2024-36302	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2024-36303.	7.8	More Details
CVE-2022-32897	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Monterey 12.5. Processing a maliciously crafted tiff file may lead to arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36303	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2024-36302.	7.8	More Details
CVE-2024-27817	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.6.7, macOS Monterey 12.7.5, iOS 16.7.8 and iPadOS 16.7.8, tvOS 17.5, visionOS 1.2, iOS 17.5 and iPadOS 17.5, macOS Sonoma 14.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2024-30369	A10 Thunder ADC Incorrect Permission Assignment Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of A10 Thunder ADC. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the installer. The issue results from incorrect permissions on a file. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of root. Was ZDI-CAN-22754.	7.8	More Details
CVE-2024-30374	Luxion KeyShot Viewer KSP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Luxion KeyShot Viewer. 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 parsing of KSP files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-22449.	7.8	More Details
CVE-2022-48683	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13. An app may be able to break out of its sandbox.	7.8	More Details
CVE-2024-30375	Luxion KeyShot Viewer KSP File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Luxion KeyShot Viewer. 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 parsing of KSP files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-22515.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27815	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in tvOS 17.5, visionOS 1.2, iOS 17.5 and iPadOS 17.5, watchOS 10.5, macOS Sonoma 14.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2024-36304	A Time-of-Check Time-Of-Use vulnerability in the Trend Micro Apex One and Apex One as a Service agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2024-36305	A security agent link following vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2024-36358	A link following vulnerability in Trend Micro Deep Security 20.x agents below build 20.0.1-3180 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2024-37289	An improper access control vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2024-27811	The issue was addressed with improved checks. This issue is fixed in tvOS 17.5, visionOS 1.2, iOS 17.5 and iPadOS 17.5, watchOS 10.5, macOS Sonoma 14.5. An app may be able to elevate privileges.	7.8	More Details
CVE-2024-27802	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.6.7, macOS Monterey 12.7.5, iOS 16.7.8 and iPadOS 16.7.8, tvOS 17.5, visionOS 1.2, iOS 17.5 and iPadOS 17.5, macOS Sonoma 14.5. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2024-27836	The issue was addressed with improved checks. This issue is fixed in visionOS 1.2, macOS Sonoma 14.5, iOS 17.5 and iPadOS 17.5. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3095	A Server-Side Request Forgery (SSRF) vulnerability exists in the Web Research Retriever component of langchain-ai/langchain version 0.1.5. The vulnerability arises because the Web Research Retriever does not restrict requests to remote internet addresses, allowing it to reach local addresses. This flaw enables attackers to execute port scans, access local services, and in some scenarios, read instance metadata from cloud environments. The vulnerability is particularly concerning as it can be exploited to abuse the Web Explorer server as a proxy for web attacks on third parties and interact with servers in the local network, including reading their response data. This could potentially lead to arbitrary code execution, depending on the nature of the local services. The vulnerability is limited to GET requests, as POST requests are not possible, but the impact on confidentiality, integrity, and availability is significant due to the potential for stolen credentials and state-changing interactions with internal APIs.	7.7	More Details
CVE-2024-4851	A Server-Side Request Forgery (SSRF) vulnerability exists in the stangirard/quivr application, version 0.0.204, which allows attackers to access internal networks. The vulnerability is present in the crawl endpoint where the 'url' parameter can be manipulated to send HTTP requests to arbitrary URLs, thereby facilitating SSRF attacks. The affected code is located in the backend/routes/crawl_routes.py file, specifically within the crawl_endpoint function. This issue could allow attackers to interact with internal services that are accessible from the server hosting the application.	7.7	More Details
CVE-2024-36414	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, a vulnerability in the connectors file verification allows for a server-side request forgery attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	7.7	More Details
CVE-2024-32703	Missing Authorization vulnerability in reputeinfosystems ARForms.This issue affects ARForms: from n/a through 6.4.	7.7	More Details
CVE-2024-5526	Grafana OnCall is an easy-to-use on-call management tool that will help reduce toil in on-call management through simpler workflows and interfaces that are tailored specifically for engineers. Grafana OnCall, from version 1.1.37 before 1.5.2 are vulnerable to a Server Side Request Forgery (SSRF) vulnerability in the webhook functionallity. This issue was fixed in version 1.5.2	7.7	More Details
CVE-2024-5585	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix for CVE-2024-1874 does not work if the command name includes trailing spaces. Original issue: when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34800	Missing Authentication for Critical Function vulnerability in Aruphash Crafthemes Demo Import allows Functionality Misuse.This issue affects Crafthemes Demo Import: from n/a through 3.3.	7.6	More Details
CVE-2024-37150	An issue in `.npmrc` support in Deno 1.44.0 was discovered where Deno would send `.npmrc` credentials for the scope to the tarball URL when the registry provided URLs for a tarball on a different domain. All users relying on .npmrc are potentially affected by this vulnerability if their private registry references tarball URLs at a different domain. This includes usage of deno install subcommand, auto-install for npm: specifiers and LSP usage. It is recommended to upgrade to Deno 1.44.1 and if your private registry ever serves tarballs at a different domain to rotate your registry credentials.	7.6	More Details
CVE-2023-32475	Dell BIOS contains a missing support for integrity check vulnerability. An attacker with physical access to the system could potentially bypass security mechanisms to run arbitrary code on the system.	7.6	More Details
CVE-2024-33563	Missing Authorization vulnerability in 8theme XStore.This issue affects XStore: from n/a through 9.3.8.	7.6	More Details
CVE-2024-24195	robdns commit d76d2e6 was discovered to contain a misaligned address at /src/zonefile-insertion.c.	7.5	More Details
CVE-2024-4887	The Qi Addons For Elementor plugin for WordPress is vulnerable to Remote File Inclusion in all versions up to, and including, 1.7.2 via the 'behavior' attributes found in the qi_addons_for_elementor_blog_list shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to include remote files on the server, resulting in code execution. Please note that this requires an attacker to create a non-existent directory or target an instance where file_exists won't return false with a non-existent directory in the path, in order to successfully exploit.	7.5	More Details
CVE-2023-4727	A flaw was found in dogtag-pki and pki-core. The token authentication scheme can be bypassed with a LDAP injection. By passing the query string parameter sessionID=*, an attacker can authenticate with an existing session saved in the LDAP directory server, which may lead to escalation of privilege.	7.5	More Details
CVE-2024-5599	The FileOrganizer – Manage WordPress and Website Files plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.7 via the 'fileorganizer_ajax_handler' function. This makes it possible for unauthenticated attackers to extract sensitive data including backups or other sensitive information if the files have been moved to the built-in Trash folder.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5637	The Market Exporter plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'remove_files' function in all versions up to, and including, 2.0.19. This makes it possible for authenticated attackers, with Subscriber-level access and above, to use path traversal to delete arbitrary files on the server.	7.5	More Details
CVE-2024-24199	smartdns commit 54b4dc was discovered to contain a misaligned address at smartdns/src/dns.c.	7.5	More Details
CVE-2024-30101	Microsoft Office Remote Code Execution Vulnerability	7.5	More Details
CVE-2024-24198	smartdns commit 54b4dc was discovered to contain a misaligned address at smartdns/src/util.c.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37293	The AWS Deployment Framework (ADF) is a framework to manage and deploy resources across multiple AWS accounts and regions within an AWS Organization. ADF allows for staged, parallel, multi-account, cross-region deployments of applications or resources via the structure defined in AWS Organizations while taking advantage of services such as AWS CodePipeline, AWS CodeBuild, and AWS CodeCommit to alleviate the heavy lifting and management compared to a traditional CI/CD setup. ADF contains a bootstrap process that is responsible to deploy ADF's bootstrap stacks to facilitate multi-account cross-region deployments. The ADF bootstrap process relies on elevated privileges to perform this task. Two versions of the bootstrap process exist; a code-change driven pipeline using AWS CodeBuild and an event-driven state machine using AWS Lambda. If an actor has permissions to change the behavior of the CodeBuild project or the Lambda function, they would be able to escalate their privileges. Prior to version 4.0.0, the bootstrap CodeBuild role provides access to the `sts:AssumeRole` operation without further restrictions. Therefore, it is able to assume into any AWS Account in the AWS Organization with the elevated privileges provided by the cross-account access role. By default, this role is not restricted when it is created by AWS Organizations, providing Administrator level access to the AWS resources in the AWS Account. The patches for this issue are included in `aws-deployment-framework` version 4.0.0. As a temporary mitigation, add a permissions boundary to the roles created by ADF in the management account. The permissions boundary should deny all IAM and STS actions. This permissions boundary should be in place until you upgrade ADF or bootstrap a new account. While the permissions boundary is in place, the account management and bootstrapping of accounts are unable to create, update, or assume into roles. This mitigates the privilege escalation risk, but also disables ADF's ability to create, manage, and bootstrap accounts.	7.5	More Details
CVE-2024-36823	The encrypt() function of Ninja Core v7.0.0 was discovered to use a weak cryptographic algorithm, leading to a possible leakage of sensitive information.	7.5	More Details
CVE-2024-35252	Azure Storage Movement Client Library Denial of Service Vulnerability	7.5	More Details
CVE-2024-35212	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected application lacks input validation due to which an attacker can gain access to the Database entries.	7.5	More Details
CVE-2024-36827	An XML External Entity (XXE) vulnerability in the ebookmeta.get_metadata function of ebookmeta before v1.2.8 allows attackers to access sensitive information or cause a Denial of Service (DoS) via crafted XML input.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32798	Missing Authorization vulnerability in WP Travel Engine.This issue affects WP Travel Engine: from n/a through 5.8.0.	7.5	More Details
CVE-2023-51847	An issue in obgm and Libcoap v.a3ed466 allows a remote attacker to cause a denial of service via thecoap_context_t function in the src/coap_threadsafe.c:297:3 component.	7.5	More Details
CVE-2024-35754	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ovic Team Ovic Importer allows Path Traversal.This issue affects Ovic Importer: from n/a through 1.6.3.	7.5	More Details
CVE-2024-35745	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Gabriel Somoza / Joseph Fitzgibbons Strategery Migrations allows Path Traversal, File Manipulation.This issue affects Strategery Migrations: from n/a through 1.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36972	In the Linux kernel, the following vulnerability has been resolved: af_unix: Update unix_sk(sk)->oob_skb under sk_receive_queue lock. Billy Jheng Bing-Jhong reported a race between __unix_gc() and queue_oob(). __unix_gc() tries to garbage-collect close()d inflight sockets, and then if the socket has MSG_OOB in unix_sk(sk)->oob_skb, GC will drop the reference and set NULL to it locklessly. However, the peer socket still can send MSG_OOB message and queue_oob() can update unix_sk(sk)->oob_skb concurrently, leading NULL pointer dereference. [0] To fix the issue, let's update unix_sk(sk)->oob_skb under the sk_receive_queue's lock and take it everywhere we touch oob_skb. Note that we defer kfree_skb() in manage_oob() to silence lockdep false-positive (See [1]). [0]: BUG: kernel NULL pointer dereference, address: 0000000000000008 PF: supervisor write access in kernel mode PF: error_code(0x0002) - not-present page PGD 8000000009f5e067 P4D 8000000009f5e067 PUD 9f5d067 PMD 0 Oops: 0002 [#1] PREEMPT SMP PTI CPU: 3 PID: 50 Comm: kworker/3:1 Not tainted 6.9.0-rc5-00191-gd091e579b864 #110 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 Workqueue: events delayed_fput RIP: 0010:skb_dequeue (./include/linux/skbuff.h:2386 ./include/linux/skbuff.h:2402 net/core/skbuff.c:3847) Code: 39 e3 74 3e 8b 43 10 48 89 ef 83 e8 01 89 43 10 49 8b 44 24 08 49 c7 44 24 08 00 00 00 00 49 8b 14 24 49 c7 04 24 00 00 00 00 <48> 89 42 08 48 89 10 e8 e7 c5 42 00 4c 89 e0 5b 5d 41 5c c3 cc cc RSP: 0018:ffffc900001bfd48 EFLAGS: 00000002 RAX: 0000000000000000 RBX: ffff8880088f5ae8 RCX: 00000000361289f9 RDX: 0000000000000000 RSI: 0000000000000206 RDI: ffff8880088f5b00 RBP: ffff8880088f5b00 R08: 0000000000080000 R09: 0000000000000001 R10: 0000000000000003 R11: 0000000000000001 R12: ffff8880056b6a00 R13: ffff8880088f5280 R14: 0000000000000001 R15: ffff8880088f5a80 FS: 0000000000000000(0000) GS:ffff88807dd80000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000008 CR3: 0000000006314000 CR4: 00000000007506f0 PKRU: 55555554 Call Trace: <TASK> unix_release_sock (net/unix/af_unix.c:654) unix_release (net/unix/af_unix.c:1050) __sock_release (net/socket.c:660) sock_close (net/socket.c:1423) __fput (fs/file_table.c:423) delayed_fput (fs/file_table.c:444 (discriminator 3)) process_one_work (kernel/workqueue.c:3259) worker_thread (kernel/workqueue.c:3329 kernel/workqueue.c:3416) kthread (kernel/kthread.c:388) ret_from_fork (arch/x86/kernel/process.c:153) ret_from_fork_asm (arch/x86/entry/entry_64.S:257) </TASK> Modules linked in: CR2: 0000000000000008	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37880	The Kyber reference implementation before 9b8d306, when compiled by LLVM Clang through 18.x with some common optimization options, has a timing side channel that allows attackers to recover an ML-KEM 512 secret key in minutes. This occurs because poly_frommsg in poly.c does not prevent Clang from emitting a vulnerable secret-dependent branch.	7.5	More Details
CVE-2024-36471	Import functionality is vulnerable to DNS rebinding attacks between verification and processing of the URL. Project administrators can run these imports, which could cause Allura to read from internal services and expose them. This issue affects Apache Allura from 1.0.1 through 1.16.0. Users are recommended to upgrade to version 1.17.0, which fixes the issue. If you are unable to upgrade, set "disable_entry_points.allura.importers = forge-tracker, forge-discussion" in your .ini config file.	7.5	More Details
CVE-2024-37568	lepture Authlib before 1.3.1 has algorithm confusion with asymmetric public keys. Unless an algorithm is specified in a jwt.decode call, HMAC verification is allowed with any asymmetric public key. (This is similar to CVE-2022-29217 and CVE-2024-33663.)	7.5	More Details
CVE-2024-31283	Missing Authorization vulnerability in zorem Advanced Local Pickup for WooCommerce.This issue affects Advanced Local Pickup for WooCommerce: from n/a through 1.6.2.	7.5	More Details
CVE-2024-34688	Due to unrestricted access to the Meta Model Repository services in SAP NetWeaver AS Java, attackers can perform DoS attacks on the application, which may prevent legitimate users from accessing it. This can result in no impact on confidentiality and integrity but a high impact on the availability of the application.	7.5	More Details
CVE-2024-35209	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected web server is allowing HTTP methods like PUT and Delete. This could allow an attacker to modify unauthorized files.	7.5	More Details
CVE-2024-30083	Windows Standards-Based Storage Management Service Denial of Service Vulnerability	7.5	More Details
CVE-2024-37393	Multiple LDAP injections vulnerabilities exist in SecurEnvoy MFA before 9.4.514 due to improper validation of user-supplied input. An unauthenticated remote attacker could exfiltrate data from Active Directory through blind LDAP injection attacks against the DESKTOP service exposed on the /secserver HTTP endpoint. This may include ms-Mcs-AdmPwd, which has a cleartext password for the Local Administrator Password Solution (LAPS) feature.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32777	Missing Authorization vulnerability in BizSwoop a CPF Concepts, LLC Brand BizPrint.This issue affects BizPrint: from n/a through 4.3.39.	7.5	More Details
CVE-2024-33561	Missing Authorization vulnerability in 8theme XStore.This issue affects XStore: from n/a through 9.3.8.	7.5	More Details
CVE-2024-5694	An attacker could have caused a use-after-free in the JavaScript engine to read memory in the JavaScript string section of the heap. This vulnerability affects Firefox < 127.	7.5	More Details
CVE-2024-5702	Memory corruption in the networking stack could have led to a potentially exploitable crash. This vulnerability affects Firefox < 125, Firefox ESR < 115.12, and Thunderbird < 115.12.	7.5	More Details
CVE-2024-33543	Missing Authorization vulnerability in CodePeople WP Time Slots Booking Form.This issue affects WP Time Slots Booking Form: from n/a through 1.2.06.	7.5	More Details
CVE-2024-26010	A stack-based buffer overflow in Fortinet FortiPAM version 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiWeb, FortiAuthenticator, FortiSwitchManager version 7.2.0 through 7.2.3, 7.0.1 through 7.0.3, FortiOS version 7.4.0 through 7.4.3, 7.2.0 through 7.2.7, 7.0.0 through 7.0.14, 6.4.0 through 6.4.15, 6.2.0 through 6.2.16, 6.0.0 through 6.0.18, FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.9, 7.0.0 through 7.0.15, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to execute unauthorized code or commands via specially crafted packets.	7.5	More Details
CVE-2024-36650	TOTOLINK AC1200 Wireless Dual Band Gigabit Router firmware A3100R V4.1.2cu.5247_B20211129, in the cgi function `setNoticeCfg` of the file `/lib/cste_modules/system.so`, the length of the user input string `NoticeUrl` is not checked. This can lead to a buffer overflow, allowing attackers to construct malicious HTTP or MQTT requests to cause a denial-of-service attack.	7.5	More Details
CVE-2024-30070	DHCP Server Service Denial of Service Vulnerability	7.5	More Details
CVE-2024-24194	robdns commit d76d2e6 was discovered to contain a NULL pointer dereference via the item->tokens component at /src/conf-parse.c.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31243	Missing Authorization vulnerability in Bricksforge.This issue affects Bricksforge: from n/a through 2.0.17.	7.5	More Details
CVE-2024-36837	SQL Injection vulnerability in CRMEB v.5.2.2 allows a remote attacker to obtain sensitive information via the getProductList function in the ProductController.php file.	7.5	More Details
CVE-2024-36745	An issue in OneFlow-Inc. Oneflow v0.9.1 allows attackers to cause a Denial of Service (DoS) via inputting a negative value into the oneflow.index_select parameter.	7.5	More Details
CVE-2024-2548	A path traversal vulnerability exists in the parisneo/lollms-webui application, specifically within the `lollms_core/lollms/server/endpoints/lollms_binding_files_server.py` and `lollms_core/lollms/security.py` files. Due to inadequate validation of file paths between Windows and Linux environments using `Path(path).is_absolute()`, attackers can exploit this flaw to read any file on the system. This issue affects the latest version of LoLLMs running on the Windows platform. The vulnerability is triggered when an attacker sends a specially crafted request to the `/user_infos/{path:path}` endpoint, allowing the reading of arbitrary files, as demonstrated with the `win.ini` file. The issue has been addressed in version 9.5 of the software.	7.5	More Details
CVE-2024-5277	In lunary-ai/lunary version 1.2.4, a vulnerability exists in the password recovery mechanism where the reset password token is not invalidated after use. This allows an attacker who compromises the recovery token to repeatedly change the password of a victim's account. The issue lies in the backend's handling of the reset password process, where the token, once used, is not discarded or invalidated, enabling its reuse. This vulnerability could lead to unauthorized account access if an attacker obtains the recovery token.	7.5	More Details
CVE-2024-5124	A timing attack vulnerability exists in the gaizhenbiao/chuanhuchatgpt repository, specifically within the password comparison logic. The vulnerability is present in version 20240310 of the software, where passwords are compared using the '=' operator in Python. This method of comparison allows an attacker to guess passwords based on the timing of each character's comparison. The issue arises from the code segment that checks a password for a particular username, which can lead to the exposure of sensitive information to an unauthorized actor. An attacker exploiting this vulnerability could potentially guess user passwords, compromising the security of the system.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37153	Evmos is the Ethereum Virtual Machine (EVM) Hub on the Cosmos Network. There is an issue with how to liquid stake using Safe which itself is a contract. The bug only appears when there is a local state change together with an ICS20 transfer in the same function and uses the contract's balance, that is using the contract address as the sender parameter in an ICS20 transfer using the ICS20 precompile. This is in essence the "infinite money glitch" allowing contracts to double the supply of Evmos after each transaction.The issue has been patched in versions >=V18.1.0.	7.5	More Details
CVE-2024-36742	An issue in the oneflow.scatter_nd parameter OneFlow-Inc. Oneflow v0.9.1 allows attackers to cause a Denial of Service (DoS) when index parameter exceeds the range of shape.	7.5	More Details
CVE-2024-36732	An issue in OneFlow-Inc. Oneflow v0.9.1 allows attackers to cause a Denial of Service (DoS) when an empty array is processed with oneflow.tensordot.	7.5	More Details
CVE-2024-36734	Improper input validation in OneFlow-Inc. Oneflow v0.9.1 allows attackers to cause a Denial of Service (DoS) via inputting a negative value into the dim parameter.	7.5	More Details
CVE-2024-36737	Improper input validation in OneFlow-Inc. Oneflow v0.9.1 allows attackers to cause a Denial of Service (DoS) via inputting a negative value into the oneflow.full parameter.	7.5	More Details
CVE-2024-4941	A local file inclusion vulnerability exists in the JSON component of gradio-app/gradio version 4.25. The vulnerability arises from improper input validation in the `postprocess()` function within `gradio/components/json_component.py`, where a user-controlled string is parsed as JSON. If the parsed JSON object contains a `path` key, the specified file is moved to a temporary directory, making it possible to retrieve it later via the `/file=..` endpoint. This issue is due to the `processing_utils.move_files_to_cache()` function traversing any object passed to it, looking for a dictionary with a `path` key, and then copying the specified file to a temporary directory. The vulnerability can be exploited by an attacker to read files on the remote system, posing a significant security risk.	7.5	More Details
CVE-2023-49928	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, Exynos 990, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 9110, Exynos W920, Exynos Modem 5123, Exynos Modem 5300. The baseband software does not properly check states specified by the RRC. This can lead to disclosure of sensitive information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36740	An issue in OneFlow-Inc. Oneflow v0.9.1 allows attackers to cause a Denial of Service (DoS) when index as a negative number exceeds the range of size.	7.5	More Details
CVE-2024-33655	The DNS protocol in RFC 1035 and updates allows remote attackers to cause a denial of service (resource consumption) by arranging for DNS queries to be accumulated for seconds, such that responses are later sent in a pulsing burst (which can be considered traffic amplification in some cases), aka the "DNSBomb" issue.	7.5	More Details
CVE-2024-5037	A flaw was found in OpenShift's Telemeter. If certain conditions are in place, an attacker can use a forged token to bypass the issue ("iss") check during JSON web token (JWT) authentication.	7.5	More Details
CVE-2024-36730	Improper input validation in OneFlow-Inc. Oneflow v0.9.1 allows attackers to cause a Denial of Service (DoS) via inputting negative values into the oneflow.zeros/ones parameter.	7.5	More Details
CVE-2024-35178	The Jupyter Server provides the backend for Jupyter web applications. Jupyter Server on Windows has a vulnerability that lets unauthenticated attackers leak the NTLMv2 password hash of the Windows user running the Jupyter server. An attacker can crack this password to gain access to the Windows machine hosting the Jupyter server, or access other network-accessible machines or 3rd party services using that credential. Or an attacker perform an NTLM relay attack without cracking the credential to gain access to other network-accessible machines. This vulnerability is fixed in 2.14.1.	7.5	More Details
CVE-2024-4881	A path traversal vulnerability exists in the parisneo/lollms application, affecting version 9.4.0 and potentially earlier versions, but fixed in version 5.9.0. The vulnerability arises due to improper validation of file paths between Windows and Linux environments, allowing attackers to traverse beyond the intended directory and read any file on the Windows system. Specifically, the application fails to adequately sanitize file paths containing backslashes (`\`), which can be exploited to access the root directory and read, or even delete, sensitive files. This issue was discovered in the context of the `/user_infos` endpoint, where a crafted request using backslashes to reference a file (e.g., `\windows\win.ini`) could result in unauthorized file access. The impact of this vulnerability includes the potential for attackers to access sensitive information such as environment variables, database files, and configuration files, which could lead to further compromise of the system.	7.5	More Details
CVE-2024-36743	An issue in OneFlow-Inc. Oneflow v0.9.1 allows attackers to cause a Denial of Service (DoS) when an empty array is processed with oneflow.dot.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5130	An Incorrect Authorization vulnerability exists in lunary-ai/lunary versions up to and including 1.2.2, which allows unauthenticated users to delete any dataset. The vulnerability is due to the lack of proper authorization checks in the dataset deletion endpoint. Specifically, the endpoint does not verify if the provided project ID belongs to the current user, thereby allowing any dataset to be deleted without proper authentication. This issue was fixed in version 1.2.8.	7.5	More Details
CVE-2024-5552	kubeflow/kubeflow is vulnerable to a Regular Expression Denial of Service (ReDoS) attack due to inefficient regular expression complexity in its email validation mechanism. An attacker can remotely exploit this vulnerability without authentication by providing specially crafted input that causes the application to consume an excessive amount of CPU resources. This vulnerability affects the latest version of kubeflow/kubeflow, specifically within the centraldashboard-angular backend component. The impact of exploiting this vulnerability includes resource exhaustion, and service disruption.	7.5	More Details
CVE-2024-2928	A Local File Inclusion (LFI) vulnerability was identified in mlflow/mlflow, specifically in version 2.9.2, which was fixed in version 2.11.3. This vulnerability arises from the application's failure to properly validate URI fragments for directory traversal sequences such as '../'. An attacker can exploit this flaw by manipulating the fragment part of the URI to read arbitrary files on the local file system, including sensitive files like '/etc/passwd'. The vulnerability is a bypass to a previous patch that only addressed similar manipulation within the URI's query string, highlighting the need for comprehensive validation of all parts of a URI to prevent LFI attacks.	7.5	More Details
CVE-2024-4084	A Server-Side Request Forgery (SSRF) vulnerability exists in the latest version of mintplex-labs/anything-llm, allowing attackers to bypass the official fix intended to restrict access to intranet IP addresses and protocols. Despite efforts to filter out intranet IP addresses starting with 192, 172, 10, and 127 through regular expressions and limit access protocols to HTTP and HTTPS, attackers can still bypass these restrictions using alternative representations of IP addresses and accessing other ports running on localhost. This vulnerability enables attackers to access any asset on the internal network, attack web services on the internal network, scan hosts on the internal network, and potentially access AWS metadata endpoints. The vulnerability is due to insufficient validation of user-supplied URLs, which can be exploited to perform SSRF attacks.	7.5	More Details
CVE-2023-49441	dnsmasq 2.9 is vulnerable to Integer Overflow via forward_query.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28021	A vulnerability exists in the FOXMAN-UN/UNEM server that affects the message queueing mechanism’s certificate validation. If exploited an attacker could spoof a trusted entity causing a loss of confidentiality and integrity.	7.4	More Details
CVE-2024-5091	The SKT Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Age Gate and Creative Slider widgets in all versions up to, and including, 2.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.4	More Details
CVE-2024-36702	libiec61850 v1.5 was discovered to contain a heap overflow via the BerEncoder_encodeLength function at /asn1/ber_encoder.c.	7.4	More Details
CVE-2024-3667	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Link To' field of multiple widgets in all versions up to, and including, 2.4.43 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.	7.4	More Details
CVE-2024-5732	A vulnerability was found in Clash up to 0.20.1 on Windows. It has been declared as critical. This vulnerability affects unknown code of the component Proxy Port. The manipulation leads to improper authentication. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to change the configuration settings. VDB-267406 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-5745	A vulnerability was found in itsourcecode Bakery Online Ordering System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/modules/product/controller.php?action=add. 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-267414 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-5733	A vulnerability was found in itsourcecode Online Discussion Forum 1.0. It has been rated as critical. This issue affects some unknown processing of the file register_me.php. The manipulation of the argument eaddress 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-267407.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5774	A vulnerability has been found in SourceCodester Stock Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file index.php of the component Login. The manipulation of the argument username/password 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-267457 was assigned to this vulnerability.	7.3	More Details
CVE-2024-30093	Windows Storage Elevation of Privilege Vulnerability	7.3	More Details
CVE-2024-37130	Dell OpenManage Server Administrator, versions 11.0.1.0 and prior, contains a Local Privilege Escalation vulnerability via XSL Hijacking. A local low-privileged malicious user could potentially exploit this vulnerability and escalate their privilege to the admin user and gain full control of the machine. Exploitation may lead to a complete system compromise.	7.3	More Details
CVE-2024-5653	A vulnerability, which was classified as critical, has been found in Chanjet Smooth T+system 3.5. This issue affects some unknown processing of the file /tplus/UFAQD/keyEdit.aspx. The manipulation of the argument KeyID 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-267185 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-37408	fprintd through 1.94.3 lacks a security attention mechanism, and thus unexpected actions might be authorized by "auth sufficient pam_fprintd.so" for Sudo. NOTE: the supplier disputes this because they believe issue resolution would involve modifying the PAM configuration to restrict pam_fprintd.so to front-ends that implement a proper attention mechanism, not modifying pam_fprintd.so or fprintd.	7.3	More Details
CVE-2024-30102	Microsoft Office Remote Code Execution Vulnerability	7.3	More Details
CVE-2024-35248	Microsoft Dynamics 365 Business Central Elevation of Privilege Vulnerability	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5225	An SQL Injection vulnerability exists in the berriai/litellm repository, specifically within the `/global/spend/logs` endpoint. The vulnerability arises due to improper neutralization of special elements used in an SQL command. The affected code constructs an SQL query by concatenating an unvalidated `api_key` parameter directly into the query, making it susceptible to SQL Injection if the `api_key` contains malicious data. This issue affects the latest version of the repository. Successful exploitation of this vulnerability could lead to unauthorized access, data manipulation, exposure of confidential information, and denial of service (DoS).	7.2	More Details
CVE-2024-1662	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in PORTY Smart Tech Technology Joint Stock Company PowerBank Application allows Retrieve Embedded Sensitive Data.This issue affects PowerBank Application: before 2.02.	7.2	More Details
CVE-2024-5542	The Master Addons – Free Widgets, Hover Effects, Toggle, Conditions, Animations for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Navigation Menu widget of the plugin's Mega Menu extension in all versions up to, and including, 2.0.6.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2024-30162	Invision Community through 4.7.16 allows remote code execution via the applications/core/modules/admin/editor/toolbar.php IPS\core\modules\admin\editor_toolbar::addPlugin() method. This method handles uploaded ZIP files that are extracted into the applications/core/interface/ckeditor/ckeditor/plugins/ directory without properly verifying their content. This can be exploited by admin users (with the toolbar_manage permission) to write arbitrary PHP files into that directory, leading to execution of arbitrary PHP code in the context of the web server user.	7.2	More Details
CVE-2024-2087	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form name values in all versions up to, and including, 2.4.43 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4902	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to time-based SQL Injection via the ‘course_id’ parameter in all versions up to, and including, 2.7.1 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 admin access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.2	More Details
CVE-2024-4889	A code injection vulnerability exists in the berriai/litellm application, version 1.34.6, due to the use of unvalidated input in the eval function within the secret management system. This vulnerability requires a valid Google KMS configuration file to be exploitable. Specifically, by setting the `UI_LOGO_PATH` variable to a remote server address in the `get_image` function, an attacker can write a malicious Google KMS configuration file to the `cached_logo.jpg` file. This file can then be used to execute arbitrary code by assigning malicious code to the `SAVE_CONFIG_TO_DB` environment variable, leading to full system control. The vulnerability is contingent upon the use of the Google KMS feature.	7.2	More Details
CVE-2024-37295	Aimeos is an Open Source e-commerce framework for online shops. Starting in version 2024.01.1 and prior to version 2024.04.5, a user with administrative privileges can upload files that look like images but contain PHP code which can then be executed in the context of the web server. Version 2024.04.5 fixes the issue.	7.2	More Details
CVE-2024-20404	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct an SSRF attack on an affected system. This vulnerability is due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain limited sensitive information for services that are associated to the affected device.	7.2	More Details
CVE-2024-36774	An arbitrary file upload vulnerability in Monstra CMS v3.0.4 allows attackers to execute arbitrary code via uploading a crafted PHP file.	7.2	More Details
CVE-2024-35730	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in realmag777 Active Products Tables for WooCommerce allows Reflected XSS.This issue affects Active Products Tables for WooCommerce: from n/a through 1.0.6.3.	7.1	More Details
CVE-2024-35697	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThimPress Eduma allows Reflected XSS.This issue affects Eduma: from n/a through 5.4.7.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35687	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Yannick Lefebvre Link Library link-library allows Reflected XSS.This issue affects Link Library: from n/a through 7.6.3.	7.1	More Details
CVE-2024-35254	Azure Monitor Agent Elevation of Privilege Vulnerability	7.1	More Details
CVE-2024-35693	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Code for Recovery 12 Step Meeting List allows Reflected XSS.This issue affects 12 Step Meeting List: from n/a through 3.14.33.	7.1	More Details
CVE-2024-35696	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Fahad Mahmood WP Docs allows Reflected XSS.This issue affects WP Docs: from n/a through 2.1.3.	7.1	More Details
CVE-2024-35718	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tribulant Newsletters allows Reflected XSS.This issue affects Newsletters: from n/a through 4.9.5.	7.1	More Details
CVE-2024-35679	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in GiveWP allows Reflected XSS.This issue affects GiveWP: from n/a through 3.12.0.	7.1	More Details
CVE-2024-31304	Missing Authorization vulnerability in MultiVendorX WC Marketplace.This issue affects WC Marketplace: from n/a through 4.1.3.	7.1	More Details
CVE-2022-48578	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Monterey 12.5. Processing an AppleScript may result in unexpected termination or disclosure of process memory.	7.1	More Details
CVE-2024-35706	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Team Heateor Heateor Social Login allows Cross-Site Scripting (XSS).This issue affects Heateor Social Login: from n/a through 1.1.32.	7.1	More Details
CVE-2024-35737	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Loopus WP Visitors Tracker allows Reflected XSS.This issue affects WP Visitors Tracker: from n/a through 2.3.	7.1	More Details
CVE-2024-35733	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in RLDD Auto Coupons for WooCommerce allows Reflected XSS.This issue affects Auto Coupons for WooCommerce: from n/a through 3.0.14.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35734	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CodePeople WP Time Slots Booking Form allows Stored XSS.This issue affects WP Time Slots Booking Form: from n/a through 1.2.10.	7.1	More Details
CVE-2024-35694	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPMobile.App allows Reflected XSS.This issue affects WPMobile.App: from n/a through 11.41.	7.1	More Details
CVE-2024-1940	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via post content in all versions up to, and including, 2.4.41 due to insufficient input sanitization performed only on the client side and insufficient output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.1	More Details
CVE-2024-32704	Missing Authorization vulnerability in reputeinfosystems ARForms.This issue affects ARForms: from n/a through 6.4.	7.1	More Details
CVE-2024-32705	Missing Authorization vulnerability in reputeinfosystems ARForms.This issue affects ARForms: from n/a through 6.4.	7.1	More Details
CVE-2024-30084	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-35265	Windows Perception Service Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-30099	Windows Kernel Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-5102	A sym-linked file accessed via the repair function in Avast Antivirus <24.2 on Windows may allow user to elevate privilege to delete arbitrary files or run processes as NT AUTHORITY\SYSTEM. The vulnerability exists within the "Repair" (settings -> troubleshooting -> repair) feature, which attempts to delete a file in the current user's AppData directory as NT AUTHORITY\SYSTEM. A low-privileged user can make a pseudo-symlink and a junction folder and point to a file on the system. This can provide a low-privileged user an Elevation of Privilege to win a race-condition which will re-create the system files and make Windows callback to a specially-crafted file which could be used to launch a privileged shell instance. This issue affects Avast Antivirus prior to 24.2.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30090	Microsoft Streaming Service Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-30088	Windows Kernel Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-5700	Memory safety bugs present in Firefox 126, Firefox ESR 115.11, and Thunderbird 115.11. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 127, Firefox ESR < 115.12, and Thunderbird < 115.12.	7.0	More Details
CVE-2024-31958	An issue was discovered in Samsung Mobile Processor EExynos 2200, Exynos 1480, Exynos 2400. It lacks a check for the validation of native handles, which can result in an Out-of-Bounds Write.	6.8	More Details
CVE-2024-5481	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.8.23 via the esc_dir function. This makes it possible for authenticated attackers to cut and paste (copy) the contents of arbitrary files on the server, which can contain sensitive information, and to cut (delete) arbitrary directories, including the root WordPress directory. By default this can be exploited by administrators only. In the premium version of the plugin, administrators can give gallery edit permissions to lower level users, which might make this exploitable by users as low as contributors.	6.8	More Details
CVE-2024-37364	Ariane Allegro Scenario Player through 2024-03-05, when Ariane Duo kiosk mode is used, allows physically proximate attackers to obtain sensitive information (such as hotel invoice content with PII), and potentially create unauthorized room keys, by entering a guest-search quote character and then accessing the underlying Windows OS.	6.8	More Details
CVE-2022-37019	Potential vulnerabilities have been identified in the system BIOS for certain HP PC products which may allow escalation of privileges and code execution. HP is releasing firmware updates to mitigate the potential vulnerabilities.	6.8	More Details
CVE-2024-36821	Insecure permissions in Linksys Velop WiFi 5 (WHW01v1) 1.1.13.202617 allows attackers to escalate privileges from Guest to root.	6.8	More Details
CVE-2022-37020	Potential vulnerabilities have been identified in the system BIOS for certain HP PC products, which might allow escalation of privileges and code execution. HP is releasing firmware updates to mitigate the potential vulnerabilities.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30076	Windows Container Manager Service Elevation of Privilege Vulnerability	6.8	More Details
CVE-2024-23111	An improper neutralization of input during web page Generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiOS version 7.4.3 and below, 7.2 all versions, 7.0 all versions and FortiProxy version 7.4.2 and below, 7.2 all versions, 7.0 all versions reboot page may allow a remote privileged attacker with super-admin access to execute JavaScript code via crafted HTTP GET requests.	6.8	More Details
CVE-2024-27377	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_get_security_info_nl(), there is no input validation check on sec_info->key_info.body.pmk_info.pmk_len coming from userspace, which can lead to a heap overwrite.	6.7	More Details
CVE-2024-27379	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_subscribe_get_nl_params(), there is no input validation check on hal_req->num_intf_addr_present coming from userspace, which can lead to a heap overwrite.	6.7	More Details
CVE-2024-27376	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_subscribe_get_nl_params(), there is no input validation check on hal_req->rx_match_filter_len coming from userspace, which can lead to a heap overwrite.	6.7	More Details
CVE-2023-46720	A stack-based buffer overflow in Fortinet FortiOS version 7.4.0 through 7.4.1 and 7.2.0 through 7.2.7 and 7.0.0 through 7.0.12 and 6.4.6 through 6.4.15 and 6.2.9 through 6.2.16 and 6.0.13 through 6.0.18 allows attacker to execute unauthorized code or commands via specially crafted CLI commands.	6.7	More Details
CVE-2024-27372	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_config_get_nl_params(), there is no input validation check on disc_attr->infrastructure_ssid_len coming from userspace, which can lead to a heap overwrite.	6.7	More Details
CVE-2024-27370	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_config_get_nl_params(), there is no input validation check on hal_req->num_config_discovery_attr coming from userspace, which can lead to a heap overwrite.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27375	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_followup_get_nl_params(), there is no input validation check on hal_req->sdea_service_specific_info_len coming from userspace, which can lead to a heap overwrite.	6.7	More Details
CVE-2024-29060	Visual Studio Elevation of Privilege Vulnerability	6.7	More Details
CVE-2024-27374	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_publish_get_nl_params(), there is no input validation check on hal_req->service_specific_info_len coming from userspace, which can lead to a heap overwrite.	6.7	More Details
CVE-2024-30063	Windows Distributed File System (DFS) Remote Code Execution Vulnerability	6.7	More Details
CVE-2024-27371	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_followup_get_nl_params(), there is no input validation check on hal_req->service_specific_info_len coming from userspace, which can lead to a heap overwrite.	6.7	More Details
CVE-2024-27373	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_nan_config_get_nl_params(), there is no input validation check on disc_attr->mesh_id_len coming from userspace, which can lead to a heap overwrite.	6.7	More Details
CVE-2024-4194	The The Album and Image Gallery plus Lightbox plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.0. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	6.5	More Details
CVE-2024-34683	An authenticated attacker can upload malicious file to SAP Document Builder service. When the victim accesses this file, the attacker is allowed to access, modify, or make the related information unavailable in the victim's browser.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33001	SAP NetWeaver and ABAP platform allows an attacker to impede performance for legitimate users by crashing or flooding the service. An impact of this Denial of Service vulnerability might be long response delays and service interruptions, thus degrading the service quality experienced by legitimate users causing high impact on availability of the application.	6.5	More Details
CVE-2024-35676	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in wpecommerce Recurring PayPal Donations allows Stored XSS.This issue affects Recurring PayPal Donations: from n/a through 1.7.	6.5	More Details
CVE-2024-35695	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Fahad Mahmood WP Docs allows Stored XSS.This issue affects WP Docs: from n/a through 2.1.3.	6.5	More Details
CVE-2024-35675	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ILLID Advanced Woo Labels allows Cross-Site Scripting (XSS).This issue affects Advanced Woo Labels: from n/a through 1.93.	6.5	More Details
CVE-2024-35705	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ciprian Popescu Block for Font Awesome allows Stored XSS.This issue affects Block for Font Awesome: from n/a through 1.4.4.	6.5	More Details
CVE-2024-27812	The issue was addressed with improvements to the file handling protocol. This issue is fixed in visionOS 1.2. Processing web content may lead to a denial-of-service.	6.5	More Details
CVE-2024-27850	This issue was addressed with improvements to the noise injection algorithm. This issue is fixed in visionOS 1.2, macOS Sonoma 14.5, Safari 17.5, iOS 17.5 and iPadOS 17.5. A maliciously crafted webpage may be able to fingerprint the user.	6.5	More Details
CVE-2024-35701	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PropertyHive allows Stored XSS.This issue affects PropertyHive: from n/a through 2.0.13.	6.5	More Details
CVE-2024-35704	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPBlockArt BlockArt Blocks allows Stored XSS.This issue affects BlockArt Blocks: from n/a through 2.1.5.	6.5	More Details
CVE-2024-35703	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SinaExtra Sina Extension for Elementor allows Stored XSS.This issue affects Sina Extension for Elementor: from n/a through 3.5.3.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35702	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jewel Theme Master Addons for Elementor allows Stored XSS.This issue affects Master Addons for Elementor: from n/a through 2.0.6.0.	6.5	More Details
CVE-2024-5268	Sonos Era 100 SMB2 Message Handling Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of Sonos Era 100 smart speakers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of SMB2 messages. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-22428.	6.5	More Details
CVE-2024-35699	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in HasThemes HT Feed allows Stored XSS.This issue affects HT Feed: from n/a through 1.2.8.	6.5	More Details
CVE-2024-27838	The issue was addressed by adding additional logic. This issue is fixed in tvOS 17.5, iOS 16.7.8 and iPadOS 16.7.8, visionOS 1.2, Safari 17.5, iOS 17.5 and iPadOS 17.5, watchOS 10.5, macOS Sonoma 14.5. A maliciously crafted webpage may be able to fingerprint the user.	6.5	More Details
CVE-2024-27830	This issue was addressed through improved state management. This issue is fixed in tvOS 17.5, visionOS 1.2, Safari 17.5, iOS 17.5 and iPadOS 17.5, watchOS 10.5, macOS Sonoma 14.5. A maliciously crafted webpage may be able to fingerprint the user.	6.5	More Details
CVE-2024-31399	Excessive platform resource consumption within a loop issue exists in Cybozu Garoon 5.0.0 to 5.15.2. If this vulnerability is exploited, processing a crafted mail may cause a denial-of-service (DoS) condition.	6.5	More Details
CVE-2024-32805	Missing Authorization vulnerability in Social Snap.This issue affects Social Snap: from n/a through 1.3.5.	6.5	More Details
CVE-2024-34691	Manage Incoming Payment Files (F1680) of SAP S/4HANA does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. As a result, it has high impact on integrity and no impact on the confidentiality and availability of the system.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5692	On Windows 10, when using the 'Save As' functionality, an attacker could have tricked the browser into saving the file with a disallowed extension such as `.url` by including an invalid character in the extension. *Note:* This issue only affected Windows operating systems. Other operating systems are unaffected. This vulnerability affects Firefox < 127, Firefox ESR < 115.12, and Thunderbird < 115.12.	6.5	More Details
CVE-2024-30481	Broken Access Control vulnerability in Samuel Marshall JCH Optimize.This issue affects JCH Optimize: from n/a through 4.0.0.	6.5	More Details
CVE-2024-30470	Missing Authorization vulnerability in YITH YITH WooCommerce Account Funds Premium.This issue affects YITH WooCommerce Account Funds Premium: from n/a through 1.33.0.	6.5	More Details
CVE-2024-30467	Missing Authorization vulnerability in WPDeveloper Essential Blocks for Gutenberg.This issue affects Essential Blocks for Gutenberg: from n/a through 4.4.9.	6.5	More Details
CVE-2024-30465	Missing Authorization vulnerability in Pagelayer Team PageLayer.This issue affects PageLayer: from n/a through 1.8.1.	6.5	More Details
CVE-2024-25929	Missing Authorization vulnerability in MultiVendorX Product Catalog Enquiry for WooCommerce by MultiVendorX.This issue affects Product Catalog Enquiry for WooCommerce by MultiVendorX: from n/a through 5.0.5.	6.5	More Details
CVE-2024-35211	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected web server, after a successful login, sets the session cookie on the browser, without applying any security attributes (such as “Secure”, “HttpOnly”, or “SameSite”).	6.5	More Details
CVE-2024-35210	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected web server is not enforcing HSTS. This could allow an attacker to perform downgrade attacks exposing confidential information.	6.5	More Details
CVE-2023-34003	Missing Authorization vulnerability in Woo WooCommerce Box Office.This issue affects WooCommerce Box Office: from n/a through 1.1.51.	6.5	More Details
CVE-2023-23775	Multiple improper neutralization of special elements used in SQL commands ('SQL Injection') vulnerabilities [CWE-89] in FortiSOAR 7.2.0 and before 7.0.3 may allow an authenticated attacker to execute unauthorized code or commands via specifically crafted strings parameters.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52199	Missing Authorization vulnerability in Matthias Pfefferle & Automattic ActivityPub.This issue affects ActivityPub: from n/a through 1.0.5.	6.5	More Details
CVE-2024-2035	An improper authorization vulnerability exists in the zenml-io/zenml repository, specifically within the API PUT /api/v1/users/id endpoint. This vulnerability allows any authenticated user to modify the information of other users, including changing the `active` status of user accounts to false, effectively deactivating them. This issue affects version 0.55.3 and was fixed in version 0.56.2. The impact of this vulnerability is significant as it allows for the deactivation of admin accounts, potentially disrupting the functionality and security of the application.	6.5	More Details
CVE-2024-5184	The EmailGPT service contains a prompt injection vulnerability. The service uses an API service that allows a malicious user to inject a direct prompt and take over the service logic. Attackers can exploit the issue by forcing the AI service to leak the standard hard-coded system prompts and/or execute unwanted prompts. When engaging with EmailGPT by submitting a malicious prompt that requests harmful information, the system will respond by providing the requested data. This vulnerability can be exploited by any individual with access to the service.	6.5	More Details
CVE-2024-35716	Missing Authorization vulnerability in Copymatic Copymatic – AI Content Writer & Generator.This issue affects Copymatic – AI Content Writer & Generator: from n/a through 1.9.	6.5	More Details
CVE-2024-35660	Missing Authorization vulnerability in Jewel Theme Master Addons for Elementor.This issue affects Master Addons for Elementor: from n/a through 2.0.5.4.1.	6.5	More Details
CVE-2023-45188	IBM Engineering Lifecycle Optimization Publishing 7.0.2 and 7.03 could allow a remote attacker to upload arbitrary files, caused by the improper validation of file extensions. By sending a specially crafted request, a remote attacker could exploit this vulnerability to upload a malicious file, which could allow the attacker to execute arbitrary code on the vulnerable system. IBM X-Force ID: 268751.	6.5	More Details
CVE-2024-34820	Missing Authorization vulnerability in If So Plugin If-So Dynamic Content Personalization.This issue affects If-So Dynamic Content Personalization: from n/a through 1.7.1.	6.5	More Details
CVE-2020-11843	This allows the information exposure to unauthorized users. This issue affects NetIQ Access Manager using version 4.5 or before	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31400	Insertion of sensitive information into sent data issue exists in Cybozu Garoon 5.0.0 to 5.15.0. If this vulnerability is exploited, unintended data may be left in forwarded mail.	6.5	More Details
CVE-2024-3504	An improper access control vulnerability exists in lunary-ai/lunary versions up to and including 1.2.2, where an admin can update any organization user to the organization owner. This vulnerability allows the elevated user to delete projects within the organization. The issue is resolved in version 1.2.7.	6.5	More Details
CVE-2024-30534	Missing Authorization vulnerability in typps Calendarista Basic Edition.This issue affects Calendarista Basic Edition: from n/a through 3.0.5.	6.5	More Details
CVE-2023-52232	Missing Authorization vulnerability in Pluggabl LLC Booster Plus for WooCommerce.This issue affects Booster Plus for WooCommerce: from n/a before 7.1.2.	6.5	More Details
CVE-2023-52230	Missing Authorization vulnerability in Pluggabl LLC Booster Plus for WooCommerce.This issue affects Booster Plus for WooCommerce: from n/a before 7.1.3.	6.5	More Details
CVE-2024-26330	An issue was discovered in Kape CyberGhostVPN 8.4.3.12823 on Windows. After a successful logout, user credentials remain in memory while the process is still open, and can be obtained by dumping the process memory and parsing it.	6.5	More Details
CVE-2024-35719	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MagniGenie RestroPress allows Stored XSS.This issue affects RestroPress: from n/a through 3.1.2.1.	6.5	More Details
CVE-2024-35691	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Marketing Fire, LLC Widget Options - Extended.This issue affects Widget Options - Extended: from n/a through 5.1.0.	6.5	More Details
CVE-2024-35688	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jewel Theme Master Addons for Elementor allows Stored XSS.This issue affects Master Addons for Elementor: from n/a through 2.0.5.9.	6.5	More Details
CVE-2024-35755	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in El tiempo Weather Widget Pro allows Stored XSS.This issue affects Weather Widget Pro: from n/a through 1.1.40.	6.5	More Details
CVE-2024-35753	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in TemplatesNext TemplatesNext OnePager allows Stored XSS.This issue affects TemplatesNext OnePager: from n/a through 1.3.3.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5654	The CF7 Google Sheets Connector plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'execute_post_data_cg7_free' function in all versions up to, and including, 5.0.9. This makes it possible for unauthenticated attackers to toggle site configuration settings, including WP_DEBUG, WP_DEBUG_LOG, SCRIPT_DEBUG, and SAVEQUERIES.	6.5	More Details
CVE-2024-5786	Cross-Site Request Forgery vulnerability in Comtrend router WLD71-T1_v2.0.201820, affecting the GRG-4280us version. This vulnerability allows an attacker to force an end user to execute unwanted actions in a web application to which he is authenticated.	6.5	More Details
CVE-2022-45168	An issue was discovered in LIVEBOX Collaboration vDesk through v018. A Bypass of Two-Factor Authentication can occur under the /login/backup_code endpoint and the /api/v1/vdeskintegration/createbackupcodes endpoint, because the application allows a user to generate or regenerate the backup codes before checking the TOTP.	6.5	More Details
CVE-2024-31612	Emlog pro2.3 is vulnerable to Cross Site Request Forgery (CSRF) via twitter.php which can be used with a XSS vulnerability to access administrator information.	6.5	More Details
CVE-2024-3153	mintplex-labs/anything-llm is affected by an uncontrolled resource consumption vulnerability in its upload file endpoint, leading to a denial of service (DOS) condition. Specifically, the server can be shut down by sending an invalid upload request. An attacker with the ability to upload documents can exploit this vulnerability to cause a DOS condition by manipulating the upload request.	6.5	More Details
CVE-2024-3404	In gaizhenbiao/chuanhuchatgpt, specifically the version tagged as 20240121, there exists a vulnerability due to improper access control mechanisms. This flaw allows an authenticated attacker to bypass intended access restrictions and read the `history` files of other users, potentially leading to unauthorized access to sensitive information. The vulnerability is present in the application's handling of access control for the `history` path, where no adequate mechanism is in place to prevent an authenticated user from accessing another user's chat history files. This issue poses a significant risk as it could allow attackers to obtain sensitive information from the chat history of other users.	6.5	More Details
CVE-2024-34799	Missing Authorization vulnerability in Repute Infosystems BookingPress.This issue affects BookingPress: from n/a through 1.0.82.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5126	An improper access control vulnerability exists in the lunary-ai/lunary repository, specifically within the versions.patch functionality for updating prompts. Affected versions include 1.2.2 up to but not including 1.2.25. The vulnerability allows unauthorized users to update prompt details due to insufficient access control checks. This issue was addressed and fixed in version 1.2.25.	6.5	More Details
CVE-2024-5131	An Improper Access Control vulnerability exists in the lunary-ai/lunary repository, affecting versions up to and including 1.2.2. The vulnerability allows unauthorized users to view any prompts in any projects by supplying a specific prompt ID to an endpoint that does not adequately verify the ownership of the prompt ID. This issue was fixed in version 1.2.25.	6.5	More Details
CVE-2024-23669	An improper authorization in Fortinet FortiWebManager version 7.2.0 and 7.0.0 through 7.0.4 and 6.3.0 and 6.2.3 through 6.2.4 and 6.0.2 allows attacker to execute unauthorized code or commands via HTTP requests or CLI.	6.5	More Details
CVE-2024-35738	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kognetiks Kognetiks Chatbot for WordPress allows Stored XSS.This issue affects Kognetiks Chatbot for WordPress: from n/a through 1.9.8.	6.5	More Details
CVE-2024-28022	A vulnerability exists in the UNEM server / APIGateway that if exploited allows a malicious user to perform an arbitrary number of authentication attempts using different passwords, and eventually gain access to other components in the same security realm using the targeted account.	6.5	More Details
CVE-2024-5382	The Master Addons – Free Widgets, Hover Effects, Toggle, Conditions, Animations for Elementor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ma-template' REST API route in all versions up to, and including, 2.0.6.1. This makes it possible for unauthenticated attackers to create or modify existing Master Addons templates or make settings modifications related to these templates.	6.5	More Details
CVE-2024-5248	In lunary-ai/lunary version 1.2.5, an improper access control vulnerability exists due to a missing permission check in the `GET /v1/users/me/org` endpoint. The platform's role definitions restrict the `Prompt Editor` role to prompt management and project viewing/listing capabilities, explicitly excluding access to user information. However, the endpoint fails to enforce this restriction, allowing users with the `Prompt Editor` role to access the full list of users in the organization. This vulnerability allows unauthorized access to sensitive user information, violating the intended access controls.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36082	SQL injection vulnerability in Music Store - WordPress eCommerce versions prior to 1.1.14 allows a remote authenticated attacker with an administrative privilege to execute arbitrary SQL commands. Information stored in the database may be obtained or altered by the attacker.	6.5	More Details
CVE-2024-5149	The BuddyForms plugin for WordPress is vulnerable to Email Verification Bypass in all versions up to, and including, 2.8.9 via the use of an insufficiently random activation code. This makes it possible for unauthenticated attackers to bypass the email verification.	6.5	More Details
CVE-2024-35474	A Directory Traversal vulnerability in iceice666 ResourcePack Server before v1.0.8 allows a remote attacker to disclose files on the server, via setPath in ResourcePackFileServer.kt.	6.5	More Details
CVE-2024-34055	Cyrus IMAP before 3.8.3 and 3.10.x before 3.10.0-rc1 allows authenticated attackers to cause unbounded memory allocation by sending many LITERALs in a single command.	6.5	More Details
CVE-2024-5839	Inappropriate Implementation in Memory Allocator in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2022-4968	netplan leaks the private key of wireguard to local users. Versions after 1.0 are not affected.	6.5	More Details
CVE-2024-5840	Policy bypass in CORS in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2024-5843	Inappropriate implementation in Downloads in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to obfuscate security UI via a malicious file. (Chromium security severity: Medium)	6.5	More Details
CVE-2024-35731	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Moose Kenta Gutenberg Blocks Responsive Blocks and block templates library for Gutenberg Editor allows Stored XSS.This issue affects Kenta Gutenberg Blocks Responsive Blocks and block templates library for Gutenberg Editor: from n/a through 1.3.9.	6.5	More Details
CVE-2024-31284	Missing Authorization vulnerability in WPDeveloper EmbedPress.This issue affects EmbedPress: from n/a through 3.9.8.	6.5	More Details
CVE-2024-35739	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in RadiusTheme The Post Grid allows Stored XSS.This issue affects The Post Grid: from n/a through 7.7.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34765	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Sensei Sensei Pro (WC Paid Courses) allows Stored XSS.This issue affects Sensei Pro (WC Paid Courses): from n/a through 4.23.1.1.23.1.	6.5	More Details
CVE-2024-35711	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Theme Freesia Event allows Stored XSS.This issue affects Event: from n/a through 1.2.2.	6.5	More Details
CVE-2024-35709	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in POSIMYTH The Plus Addons for Elementor Page Builder Lite allows Stored XSS.This issue affects The Plus Addons for Elementor Page Builder Lite: from n/a through 5.5.4.	6.5	More Details
CVE-2024-35708	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in apollo13themes Rife Free allows Stored XSS.This issue affects Rife Free: from n/a through 2.4.19.	6.5	More Details
CVE-2024-35707	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Team Heateor Heateor Social Login allows Stored XSS.This issue affects Heateor Social Login: from n/a through 1.1.32.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36968	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix div-by-zero in l2cap_le_flowctl_init() l2cap_le_flowctl_init() can cause both div-by-zero and an integer overflow since hdev->le_mtu may not fall in the valid range. Move MTU from hci_dev to hci_conn to validate MTU and stop the connection process earlier if MTU is invalid. Also, add a missing validation in read_buffer_size() and make it return an error value if the validation fails. Now hci_conn_add() returns ERR_PTR() as it can fail due to the both a kzalloc failure and invalid MTU value. divide error: 0000 [#1] PREEMPT SMP KASAN NOPTI CPU: 0 PID: 67 Comm: kworker/u5:0 Tainted: G W 6.9.0-rc5+ #20 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: hci0 hci_rx_work RIP: 0010:l2cap_le_flowctl_init+0x19e/0x3f0 net/bluetooth/l2cap_core.c:547 Code: e8 17 17 0c 00 66 41 89 9f 84 00 00 00 bf 01 00 00 00 41 b8 02 00 00 00 4c 89 fe 4c 89 e2 89 d9 e8 27 17 0c 00 44 89 f0 31 d2 <66> f7 f3 89 c3 ff c3 4d 8d b7 88 00 00 00 4c 89 f0 48 c1 e8 03 42 RSP: 0018:ffff88810bc0f858 EFLAGS: 00010246 RAX: 00000000000002a0 RBX: 0000000000000000 RCX: dffffc0000000000 RDX: 0000000000000000 RSI: ffff88810bc0f7c0 RDI: ffffc90002dcb66f RBP: ffff88810bc0f880 R08: aa69db2dda70ff01 R09: 0000ffaaaaaaaaaa R10: 0084000000ffaaaa R11: 0000000000000000 R12: ffff88810d65a084 R13: dffffc0000000000 R14: 00000000000002a0 R15: ffff88810d65a000 FS: 0000000000000000(0000) GS:ffff88811ac00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000020000100 CR3: 0000000103268003 CR4: 0000000000770ef0 PKRU: 55555554 Call Trace: <TASK> l2cap_le_connect_req net/bluetooth/l2cap_core.c:4902 [inline] l2cap_le_sig_cmd net/bluetooth/l2cap_core.c:5420 [inline] l2cap_le_sig_channel net/bluetooth/l2cap_core.c:5486 [inline] l2cap_recv_frame+0xe59d/0x11710 net/bluetooth/l2cap_core.c:6809 l2cap_recv_acldata+0x544/0x10a0 net/bluetooth/l2cap_core.c:7506 hci_acldata_packet net/bluetooth/hci_core.c:3939 [inline] hci_rx_work+0x5e5/0xb20 net/bluetooth/hci_core.c:4176 process_one_work kernel/workqueue.c:3254 [inline] process_scheduled_works+0x90f/0x1530 kernel/workqueue.c:3335 worker_thread+0x926/0xe70 kernel/workqueue.c:3416 kthread+0x2e3/0x380 kernel/kthread.c:388 ret_from_fork+0x5c/0x90 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:244 </TASK> Modules linked in: ---[end trace 0000000000000000]---	6.5	More Details
CVE-2024-35713	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in UAPP GROUP Testimonial Carousel For Elementor allows Stored XSS.This issue affects Testimonial Carousel For Elementor: from n/a through 10.1.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27800	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.6.7, macOS Monterey 12.7.5, iOS 16.7.8 and iPadOS 16.7.8, tvOS 17.5, visionOS 1.2, iOS 17.5 and iPadOS 17.5, watchOS 10.5, macOS Sonoma 14.5. Processing a maliciously crafted message may lead to a denial-of-service.	6.5	More Details
CVE-2024-35714	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Theme Freesia Idyllic allows Stored XSS.This issue affects Idyllic: from n/a through 1.1.8.	6.5	More Details
CVE-2024-35715	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in peregrinethemes Bloglo, peregrinethemes Blogvi allows Stored XSS.This issue affects Bloglo: from n/a through 1.1.3; Blogvi: from n/a through 1.0.5.	6.5	More Details
CVE-2024-35740	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Theme Freesia Pixgraphy allows Stored XSS.This issue affects Pixgraphy: from n/a through 1.3.8.	6.5	More Details
CVE-2024-35681	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in gVectors Team wpDiscuz allows Stored XSS.This issue affects wpDiscuz: from n/a through 7.6.18.	6.5	More Details
CVE-2024-5152	The ElementsReady Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘_id’ parameter in all versions up to, and including, 6.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5224	The Easy Social Like Box – Popup – Sidebar Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'cardoza_facebook_like_box' shortcode in all versions up to, and including, 4.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4451	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's colibri_video_player shortcode in all versions up to, and including, 1.0.276 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4669	The Events Addon for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Basic Slider, Upcoming Events, and Schedule widgets in all versions up to, and including, 2.1.4 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-2024-5646	The Futurio Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘header_size’ attribute within the Advanced Text Block widget in all versions up to, and including, 2.0.5 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-2024-5530	The ShopLentor – WooCommerce Builder for Elementor & Gutenberg +12 Modules – All in One Solution (formerly WooLentor) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's WL: Product Horizontal Filter widget in all versions up to, and including, 2.9.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1164	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's contact form widget error message and redirect URL in all versions up to, and including, 2.4.43 due to insufficient input sanitization and output escaping on user supplied error messages. 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-2024-4354	The TablePress – Tables in WordPress made easy plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.3 via the get_files_to_import() function. This makes it possible for authenticated attackers, with author-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. Due to the complex nature of protecting against DNS rebind attacks in WordPress software, we settled on the developer simply restricting the usage of the URL import functionality to just administrators. While this is not optimal, we feel this poses a minimal risk to most site owners and ideally WordPress core would correct this issue in wp_safe_remote_get() and other functions.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5090	The SiteOrigin Widgets Bundle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's SiteOrigin Blog Widget in all versions up to, and including, 1.61.1 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-2024-5141	The Rotating Tweets (Twitter widget and shortcode) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's' 'rotatingtweets' in all versions up to, and including, 1.9.10 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-2024-4042	The Post Grid, Form Maker, Popup Maker, WooCommerce Blocks, Post Blocks, Post Carousel – Combo Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' attribute of the menu-wrap-item block in all versions up to, and including, 2.2.80 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-2024-5640	The Prime Slider – Addons For Elementor (Revolution of a slider, Hero Slider, Ecommerce Slider) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘id’ attribute within the Pacific widget in all versions up to, and including, 3.14.7 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-2024-5612	The Essential Addons for Elementor Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘eael_lightbox_open_btn_icon’ parameter within the Lightbox & Modal widget in all versions up to, and including, 5.8.15 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-2024-5425	The WP jQuery Lightbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘title’ attribute in all versions up to, and including, 1.5.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5342	The Simple Image Popup Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'sips_popup' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5038	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.0.276 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-2024-2922	The Themesflat Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via widget tags in all versions up to, and including, 2.1.1 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-2024-5188	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'get_manual_calendar_events' function in all versions up to, and including, 5.9.22 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-2024-5001	The Image Hover Effects for Elementor with Lightbox and Flipbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_id', 'oxi_addons_f_title_tag', and 'content_description_tag' parameters in all versions up to, and including, 3.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5317	The Newsletter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'np1' parameter in all versions up to, and including, 8.3.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1988	The Post Grid, Form Maker, Popup Maker, WooCommerce Blocks, Post Blocks, Post Carousel – Combo Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tag' attribute in blocks in all versions up to, and including, 2.2.80 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-2024-5531	The Ocean Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Flickr widget in all versions up to, and including, 2.2.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-6745	The Custom Field Template plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'cpt' shortcode in all versions up to, and including, 2.6.1 due to insufficient input sanitization and output escaping on user supplied post meta. 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-2024-1161	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Custom Attributes for blocks in all versions up to, and including, 2.4.43 due to insufficient input sanitization and output escaping. 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-2024-4705	The Testimonials Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's testimonials shortcode in all versions up to, and including, 4.0.4 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 Number	Description	Base Score	Reference
CVE-2024-4707	The Materialis Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's materialis_contact_form shortcode in all versions up to, and including, 1.3.41 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-2024-1768	The Clever Fox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's info box block in all versions up to, and including, 25.2.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2350	The Clever Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the CAFE Icon, CAFE Team Member, and CAFE Slider widgets in all versions up to, and including, 2.1.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4212	The Themesflat Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's TF Group Image, TF Nav Menu, TF Posts, TF Woo Product Grid, TF Accordion, and TF Image Box widgets in all versions up to, and including, 2.1.1 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-2024-0627	The Custom Field Template plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's custom field name column in all versions up to, and including, 2.6.1 due to insufficient input sanitization and output escaping on user supplied custom fields. 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-2024-4488	The Royal Elementor Addons and Templates for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘inline_list’ parameter in versions up to, and including, 1.3.976 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4489	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘custom_upload_mimes’ function in versions up to, and including, 1.3.976 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4364	The Qi Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's button widgets in all versions up to, and including, 1.7.2 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-2024-5189	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘custom_js’ parameter in all versions up to, and including, 5.9.23 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-2024-5663	The Cards for Beaver Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Cards widget in all versions up to, and including, 1.1.3 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-2024-4459	The Themesflat Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widget's titles in all versions up to, and including, 2.1.1 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-2024-4001	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpdm_modal_login_form' shortcode in all versions up to, and including, 3.2.93 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5162	The WordPress prettyPhoto plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘url’ parameter in all versions up to, and including, 1.2.3 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-2024-4608	The SellKit – Funnel builder and checkout optimizer for WooCommerce to sell more, faster plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 1.9.8 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-2024-5571	The EmbedPress – Embed PDF, Google Docs, Vimeo, Wistia, Embed YouTube Videos, Audios, Maps & Embed Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' attribute within the plugin's EmbedPress PDF widget in all versions up to, and including, 4.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4821	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's su_lightbox shortcode in all versions up to, and including, 7.1.6 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-2024-5221	The Qi Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploader in all versions up to, and including, 1.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4458	The Themesflat Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting in several widgets via URL parameters in all versions up to, and including, 2.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37163	SkyScrape is a GUI Dashboard for AWS Infrastructure and Managing Resources and Usage Costs. SkyScrape's API requests are currently unsecured HTTP requests, leading to potential vulnerabilities for the user's temporary credentials and data. This affects version 1.0.0.	6.4	More Details
CVE-2024-5536	The GamiPress – Link plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's gamipress_link shortcode in all versions up to, and including, 1.1.4 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-2024-5439	The Blocksy theme for WordPress is vulnerable to Reflected Cross-Site Scripting via the custom_url parameter in all versions up to, and including, 2.0.50 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.	6.4	More Details
CVE-2024-5645	The Envo Extra plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘button_css_id’ parameter within the Button widget in all versions up to, and including, 1.8.23 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-2024-4703	The One Page Express Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's one_page_express_contact_form shortcode in all versions up to, and including, 1.6.37 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5006	The Boostify Header Footer Builder for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘size’ parameter in all versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5584	The WordPress Online Booking and Scheduling Plugin – Bookly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Color Profile parameter in all versions up to, and including, 23.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with the staff member role and Subscriber-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-2024-5222	The Responsive Addons – Starter Templates, Advanced Features and Customizer Settings for Responsive Theme. plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file uploader in all versions up to, and including, 3.0.5 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-2024-5426	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘svg’ parameter in all versions up to, and including, 1.8.23 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, this can only be exploited by administrators, but the ability to use and configure Photo Gallery can be extended to contributors on pro versions of the plugin.	6.4	More Details
CVE-2024-4939	The Weaver Xtreme Theme Support plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's div shortcode in all versions up to, and including, 6.4 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-2024-5259	The MultiVendorX Marketplace – WooCommerce MultiVendor Marketplace Solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘hover_animation’ parameter in all versions up to, and including, 4.1.11 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5161	The Magical Addons For Elementor (Header Footer Builder, Free Elementor Widgets, Elementor Templates Library) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_id' parameter in all versions up to, and including, 1.1.39 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-2024-23793	The file upload feature in OTRS and ((OTRS)) Community Edition has a path traversal vulnerability. This issue permits authenticated agents or customer users to upload potentially harmful files to directories accessible by the web server, potentially leading to the execution of local code like Perl scripts. This issue affects OTRS: from 7.0.X through 7.0.49, 8.0.X, 2023.X, from 2024.X through 2024.3.2; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34.	6.3	More Details
CVE-2024-34826	Missing Authorization vulnerability in Tobias Conrad Design for Contact Form 7 Style WordPress Plugin – CF7 WOW Styler.This issue affects Design for Contact Form 7 Style WordPress Plugin – CF7 WOW Styler: from n/a through 1.6.4.	6.3	More Details
CVE-2024-5775	A vulnerability was found in SourceCodester Vehicle Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file updatebill.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-267458 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-5636	A vulnerability was found in itsourcecode Bakery Online Ordering System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file report/index.php. The manipulation of the argument procduct 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-267092.	6.3	More Details
CVE-2024-5773	A vulnerability, which was classified as critical, was found in Netentsec NS-ASG Application Security Gateway 6.3. Affected is an unknown function of the file /protocol/firewall/deletemacbind.php. The manipulation of the argument messagecontent 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-267456. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5087	The Minimal Coming Soon – Coming Soon Page plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the validate_ajax, deactivate_ajax, and save_ajax functions in all versions up to, and including, 2.38. This makes it possible for authenticated attackers, with Subscriber-level access and above, to edit the license key, which could disable features of the plugin.	6.3	More Details
CVE-2024-27885	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Sonoma 14.5, macOS Ventura 13.6.7, macOS Monterey 12.7.5. An app may be able to modify protected parts of the file system.	6.3	More Details
CVE-2024-5772	A vulnerability, which was classified as critical, has been found in Netentsec NS-ASG Application Security Gateway 6.3. This issue affects some unknown processing of the file /protocol/iscuser/deleteiscuser.php. The manipulation of the argument messagecontent 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-267455. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-5684	An attacker with access to the private network (the charger is connected to) or local access to the Ethernet-Interface can exploit a faulty implementation of the JWT-library in order to bypass the password authentication to the web configuration interface and then has full access as the user would have. However, an attacker will not have developer or admin rights. If the implementation of the JWT-library is wrongly configured to accept "none"-algorithms, the server will pass insecure JWT. A local, unauthenticated attacker can exploit this vulnerability to bypass the authentication mechanism.	6.3	More Details
CVE-2024-5771	A vulnerability classified as critical was found in LabVantage LIMS 2017. This vulnerability affects unknown code of the file /labvantage/rc?command=page&page=SampleList&_iframename=list of the component POST Request Handler. The manipulation of the argument param1 leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-267454 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-35208	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V1.2). The affected web server stored the password in cleartext. This could allow attacker in a privileged position to obtain access passwords.	6.3	More Details
CVE-2024-31307	Missing Authorization vulnerability in appscreo Easy Social Share Buttons.This issue affects Easy Social Share Buttons: from n/a through 9.4.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5734	A vulnerability classified as critical has been found in itsourcecode Online Discussion Forum 1.0. Affected is an unknown function of the file /members/poster.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. The identifier of this vulnerability is VDB-267408.	6.3	More Details
CVE-2024-27840	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.6.7, macOS Monterey 12.7.5, iOS 16.7.8 and iPadOS 16.7.8, tvOS 17.5, visionOS 1.2, iOS 17.5 and iPadOS 17.5, watchOS 10.5. An attacker that has already achieved kernel code execution may be able to bypass kernel memory protections.	6.3	More Details
CVE-2024-3716	A flaw was found in foreman-installer when puppet-candlepin is invoked cpdb with the --password parameter. This issue leaks the password in the process list and allows an attacker to take advantage and obtain the password.	6.2	More Details
CVE-2024-37156	The SuluFormBundle adds support for creating dynamic forms in Sulu Admin. The TokenController get parameter formName is not sanitized in the returned input field which leads to XSS. This vulnerability is fixed in 2.5.3.	6.1	More Details
CVE-2024-5673	Vulnerability in Dulldusk's PHP File Manager affecting version 1.7.8. This vulnerability consists of an XSS through the fm_current_dir parameter of index.php. An attacker could send a specially crafted JavaScript payload to an authenticated user and partially hijack their browser session.	6.1	More Details
CVE-2024-5478	A Cross-site Scripting (XSS) vulnerability exists in the SAML metadata endpoint `/auth/saml/${org?.id}/metadata` of lunary-ai/lunary version 1.2.7. The vulnerability arises due to the application's failure to escape or validate the `orgId` parameter supplied by the user before incorporating it into the generated response. Specifically, the endpoint generates XML responses for SAML metadata, where the `orgId` parameter is directly embedded into the XML structure without proper sanitization or validation. This flaw allows an attacker to inject arbitrary JavaScript code into the generated SAML metadata page, leading to potential theft of user cookies or authentication tokens.	6.1	More Details
CVE-2024-2383	A clickjacking vulnerability exists in zenml-io/zenml versions up to and including 0.55.5 due to the application's failure to set appropriate X-Frame-Options or Content-Security-Policy HTTP headers. This vulnerability allows an attacker to embed the application UI within an iframe on a malicious page, potentially leading to unauthorized actions by tricking users into interacting with the interface under the attacker's control. The issue was addressed in version 0.56.3.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3469	The GP Premium plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the message parameter in all versions up to, and including, 2.4.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-6956	The EasyAzon – Amazon Associates Affiliate Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'easyazon-cloaking-locale' parameter in all versions up to, and including, 5.1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-5278	gaizhenbiao/chuanhuchatgpt is vulnerable to an unrestricted file upload vulnerability due to insufficient validation of uploaded file types in its `/upload` endpoint. Specifically, the `handle_file_upload` function does not sanitize or validate the file extension or content type of uploaded files, allowing attackers to upload files with arbitrary extensions, including HTML files containing XSS payloads and Python files. This vulnerability, present in the latest version as of 20240310, could lead to stored XSS attacks and potentially result in remote code execution (RCE) on the server hosting the application.	6.1	More Details
CVE-2024-37384	Roundcube Webmail before 1.5.7 and 1.6.x before 1.6.7 allows XSS via list columns from user preferences.	6.1	More Details
CVE-2024-37383	Roundcube Webmail before 1.5.7 and 1.6.x before 1.6.7 allows XSS via SVG animate attributes.	6.1	More Details
CVE-2024-5613	The Formula theme for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'id' parameter in the 'quality_customizer_notify_dismiss_action' AJAX action in all versions up to, and including, 0.5.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-5698	By manipulating the fullscreen feature while opening a data-list, an attacker could have overlaid a text box over the address bar. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 127.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5693	Offscreen Canvas did not properly track cross-origin tainting, which could be used to access image data from another site in violation of same-origin policy. This vulnerability affects Firefox < 127, Firefox ESR < 115.12, and Thunderbird < 115.12.	6.1	More Details
CVE-2024-5638	The Formula theme for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘id’ parameter in the 'ti_customizer_notify_dismiss_recommended_plugins' AJAX action in all versions up to, and including, 0.5.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-36306	A link following vulnerability in the Trend Micro Apex One and Apex One as a Service Damage Cleanup Engine could allow a local attacker to create a denial-of-service condition on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	6.1	More Details
CVE-2024-34686	Due to insufficient input validation, SAP CRM WebClient UI allows an unauthenticated attacker to craft a URL link which embeds a malicious script. When a victim clicks on this link, the script will be executed in the victim's browser giving the attacker the ability to access and/or modify information with no effect on availability of the application.	6.1	More Details
CVE-2024-27380	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_set_delayed_wakeup_type(), there is no input validation check on a length of ioctl_args->args[i] coming from userspace, which can lead to a heap over-read.	6.0	More Details
CVE-2024-27381	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_send_action_frame_ut(), there is no input validation check on len coming from userspace, which can lead to a heap over-read.	6.0	More Details
CVE-2024-27382	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_send_action_frame(), there is no input validation check on len coming from userspace, which can lead to a heap over-read.	6.0	More Details
CVE-2024-27378	An issue was discovered in Samsung Mobile Processor Exynos 980, Exynos 850, Exynos 1280, Exynos 1380, and Exynos 1330. In the function slsi_send_action_frame_cert(), there is no input validation check on len coming from userspace, which can lead to a heap over-read.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33500	A vulnerability has been identified in Mendix Applications using Mendix 10 (All versions < V10.11.0), Mendix Applications using Mendix 10 (V10.6) (All versions < V10.6.9), Mendix Applications using Mendix 9 (All versions >= V9.3.0 < V9.24.22). Affected applications could allow users with the capability to manage a role to elevate the access rights of users with that role. Successful exploitation requires to guess the id of a target role which contains the elevated access rights.	5.9	More Details
CVE-2024-28818	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, Exynos 990, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 2400, Exynos Modem 5123, Exynos Modem 5300. The baseband software does not properly check states specified by the RRC (Radio Resource Control) module. This can lead to disclosure of sensitive information.	5.9	More Details
CVE-2024-35732	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in YITH YITH Custom Login allows Stored XSS.This issue affects YITH Custom Login: from n/a through 1.7.0.	5.9	More Details
CVE-2024-36405	liboqs is a C-language cryptographic library that provides implementations of post-quantum cryptography algorithms. A control-flow timing lean has been identified in the reference implementation of the Kyber key encapsulation mechanism when it is compiled with Clang 15-18 for `-Os`, `-O1`, and other compilation options. A proof-of-concept local attack on the reference implementation leaks the entire ML-KEM 512 secret key in ~10 minutes using end-to-end decapsulation timing measurements. The issue has been fixed in version 0.10.1. As a possible workaround, some compiler options may produce vectorized code that does not leak secret information, however relying on these compiler options as a workaround may not be reliable.	5.9	More Details
CVE-2024-22279	Improper handling of requests in Routing Release > v0.273.0 and <= v0.297.0 allows an unauthenticated attacker to degrade the service availability of the Cloud Foundry deployment if performed at scale.	5.9	More Details
CVE-2024-35751	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Creative Motion, Will Bontrager Software, LLC Woody ad snippets allows Stored XSS.This issue affects Woody ad snippets: from n/a through 2.4.10.	5.9	More Details
CVE-2024-3049	A flaw was found in Booth, a cluster ticket manager. If a specially-crafted hash is passed to gcry_md_get_algo_dlen(), it may allow an invalid HMAC to be accepted by the Booth server.	5.9	More Details
CVE-2024-35752	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Enea Overclokk Stellissimo Text Box allows Stored XSS.This issue affects Stellissimo Text Box: from n/a through 1.1.4.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35756	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CeiKay Tooltip CK tooltip-ck allows Stored XSS.This issue affects Tooltip CK: from n/a through 2.2.15.	5.9	More Details
CVE-2024-28833	Improper restriction of excessive authentication attempts with two factor authentication methods in Checkmk 2.3 before 2.3.0p6 facilitates brute-forcing of second factor mechanisms.	5.9	More Details
CVE-2024-35698	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in YITH YITH WooCommerce Tab Manager allows Stored XSS.This issue affects YITH WooCommerce Tab Manager: from n/a through 1.35.0.	5.9	More Details
CVE-2024-5813	A medium severity vulnerability in BIPS has been identified where an authenticated attacker with high privileges can access the SSH private keys via an information leak in the server response.	5.9	More Details
CVE-2024-2408	The openssl_private_decrypt function in PHP, when using PKCS1 padding (OPENSSL_PKCS1_PADDING, which is the default), is vulnerable to the Marvin Attack unless it is used with an OpenSSL version that includes the changes from this pull request: https://github.com/openssl/openssl/pull/13817 (rsa_pkcs1_implicit_rejection). These changes are part of OpenSSL 3.2 and have also been backported to stable versions of various Linux distributions, as well as to the PHP builds provided for Windows since the previous release. All distributors and builders should ensure that this version is used to prevent PHP from being vulnerable. PHP Windows builds for the versions 8.1.29, 8.2.20 and 8.3.8 and above include OpenSSL patches that fix the vulnerability.	5.9	More Details
CVE-2024-36417	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. Prior to versions 7.14.4 and 8.6.1, an unverified IFrame can be added some some inputs, which could allow for a cross-site scripting attack. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	5.7	More Details
CVE-2024-36531	nukeviet v.4.5 and before and nukeviet-egov v.1.2.02 and before are vulnerable to arbitrary code execution via the /admin/extensions/upload.php component.	5.7	More Details
CVE-2024-28023	A vulnerability exists in the message queueing mechanism that if exploited can lead to the exposure of resources or functionality to unintended actors, possibly providing attackers with sensitive information or even execute arbitrary code.	5.7	More Details
CVE-2024-35263	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4013	A bug exists in the API, mesh_node_power_off(), which fails to copy the contents of the Replay Protection List (RPL) from RAM to NVM before powering down, resulting in the ability to replay unsaved messages. Note that as of June 2024, the Gecko SDK was renamed to the Simplicity SDK, and the versioning scheme was changed from Gecko SDK vX.Y.Z to Simplicity SDK YYYY.MM.Patch#.	5.6	More Details
CVE-2024-35255	Azure Identity Libraries and Microsoft Authentication Library Elevation of Privilege Vulnerability	5.5	More Details
CVE-2024-30096	Windows Cryptographic Services Information Disclosure Vulnerability	5.5	More Details
CVE-2024-27844	The issue was addressed with improved checks. This issue is fixed in visionOS 1.2, macOS Sonoma 14.5, Safari 17.5. A website's permission dialog may persist after navigation away from the site.	5.5	More Details
CVE-2024-23282	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.5, watchOS 10.5, iOS 17.5 and iPadOS 17.5, iOS 16.7.8 and iPadOS 16.7.8. A maliciously crafted email may be able to initiate FaceTime calls without user authorization.	5.5	More Details
CVE-2023-40389	The issue was addressed with improved restriction of data container access. This issue is fixed in macOS Ventura 13.6.5, macOS Monterey 12.7.4. An app may be able to access sensitive user data.	5.5	More Details
CVE-2024-27792	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in macOS Sonoma 14.4. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-24789	The archive/zip package's handling of certain types of invalid zip files differs from the behavior of most zip implementations. This misalignment could be exploited to create an zip file with contents that vary depending on the implementation reading the file. The archive/zip package now rejects files containing these errors.	5.5	More Details
CVE-2024-30067	Winlogon Elevation of Privilege Vulnerability	5.5	More Details
CVE-2024-30066	Winlogon Elevation of Privilege Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27805	An issue was addressed with improved validation of environment variables. This issue is fixed in macOS Ventura 13.6.7, macOS Monterey 12.7.5, iOS 16.7.8 and iPadOS 16.7.8, tvOS 17.5, iOS 17.5 and iPadOS 17.5, watchOS 10.5, macOS Sonoma 14.5. An app may be able to access sensitive user data.	5.5	More Details
CVE-2024-27806	This issue was addressed with improved environment sanitization. This issue is fixed in macOS Ventura 13.6.7, macOS Monterey 12.7.5, iOS 16.7.8 and iPadOS 16.7.8, tvOS 17.5, iOS 17.5 and iPadOS 17.5, watchOS 10.5, macOS Sonoma 14.5. An app may be able to access sensitive user data.	5.5	More Details
CVE-2024-30065	Windows Themes Denial of Service Vulnerability	5.5	More Details
CVE-2024-37294	Aimeos is an Open Source e-commerce framework for online shops. All SaaS and marketplace setups using Aimeos version from 2022/2023/2024 are affected by a potential denial of service attack. Users should upgrade to versions 2022.10.17, 2023.10.17, or 2024.04 of the aimeos/aimeos-core package to receive a patch.	5.5	More Details
CVE-2024-37176	SAP BW/4HANA Transformation and Data Transfer Process (DTP) allows an authenticated attacker to gain higher access levels than they should have by exploiting improper authorization checks. This results in escalation of privileges. It has no impact on the confidentiality of data but may have low impacts on the integrity and availability of the application.	5.5	More Details
CVE-2024-22525	dnspod-sr 0dfbd37 contains a SEGV.	5.5	More Details
CVE-2024-22524	dnspod-sr 0dfbd37 is vulnerable to buffer overflow.	5.5	More Details
CVE-2024-36965	In the Linux kernel, the following vulnerability has been resolved: remoteproc: mediatek: Make sure IPI buffer fits in L2TCM The IPI buffer location is read from the firmware that we load to the System Companion Processor, and it's not granted that both the SRAM (L2TCM) size that is defined in the devicetree node is large enough for that, and while this is especially true for multi-core SCP, it's still useful to check on single-core variants as well. Failing to perform this check may make this driver perform R/W operations out of the L2TCM boundary, resulting (at best) in a kernel panic. To fix that, check that the IPI buffer fits, otherwise return a failure and refuse to boot the relevant SCP core (or the SCP at all, if this is single core).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36967	In the Linux kernel, the following vulnerability has been resolved: KEYS: trusted: Fix memory leak in tpm2_key_encode() 'scratch' is never freed. Fix this by calling kfree() in the success, and in the error case.	5.5	More Details
CVE-2024-36969	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix division by zero in setup_dsc_config When slice_height is 0, the division by slice_height in the calculation of the number of slices will cause a division by zero driver crash. This leaves the kernel in a state that requires a reboot. This patch adds a check to avoid the division by zero. The stack trace below is for the 6.8.4 Kernel. I reproduced the issue on a Z16 Gen 2 Lenovo Thinkpad with a Apple Studio Display monitor connected via Thunderbolt. The amdgpu driver crashed with this exception when I rebooted the system with the monitor connected. kernel: ? die (arch/x86/kernel/dumpstack.c:421 arch/x86/kernel/dumpstack.c:434 arch/x86/kernel/dumpstack.c:447) kernel: ? do_trap (arch/x86/kernel/traps.c:113 arch/x86/kernel/traps.c:154) kernel: ? setup_dsc_config (drivers/gpu/drm/amd/amdgpu/../display/dc/dsc/dc_dsc.c:1053) amdgpu kernel: ? do_error_trap (./arch/x86/include/asm/traps.h:58 arch/x86/kernel/traps.c:175) kernel: ? setup_dsc_config (drivers/gpu/drm/amd/amdgpu/../display/dc/dsc/dc_dsc.c:1053) amdgpu kernel: ? exc_divide_error (arch/x86/kernel/traps.c:194 (discriminator 2)) kernel: ? setup_dsc_config (drivers/gpu/drm/amd/amdgpu/../display/dc/dsc/dc_dsc.c:1053) amdgpu kernel: ? asm_exc_divide_error (./arch/x86/include/asm/idtentry.h:548) kernel: ? setup_dsc_config (drivers/gpu/drm/amd/amdgpu/../display/dc/dsc/dc_dsc.c:1053) amdgpu kernel: dc_dsc_compute_config (drivers/gpu/drm/amd/amdgpu/../display/dc/dsc/dc_dsc.c:1109) amdgpu After applying this patch, the driver no longer crashes when the monitor is connected and the system is rebooted. I believe this is the same issue reported for 3113.	5.5	More Details
CVE-2024-31613	BOSSCMS v3.10 is vulnerable to Cross Site Request Forgery (CSRF) in name="head_code" or name="foot_code."	5.4	More Details
CVE-2024-34815	Missing Authorization vulnerability in Codection Import and export users and customers.This issue affects Import and export users and customers: from n/a through 1.26.5.	5.4	More Details
CVE-2024-21751	Missing Authorization vulnerability in RabbitLoader.This issue affects RabbitLoader: from n/a through 2.19.13.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35662	Missing Authorization vulnerability in Andreas Sofantzis Simple COD Fees for WooCommerce.This issue affects Simple COD Fees for WooCommerce: from n/a through 2.0.2.	5.4	More Details
CVE-2024-2017	The Countdown, Coming Soon, Maintenance – Countdown & Clock plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the conditionsRow and switchCountdown functions in all versions up to, and including, 2.7.8. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject PHP Objects and modify the status of countdowns.	5.4	More Details
CVE-2024-5127	In lunary-ai/lunary versions 1.2.2 through 1.2.25, an improper access control vulnerability allows users on the Free plan to invite other members and assign them any role, including those intended for Paid and Enterprise plans only. This issue arises due to insufficient backend validation of roles and permissions, enabling unauthorized users to join a project and potentially exploit roles and permissions not intended for their use. The vulnerability specifically affects the Team feature, where the backend fails to validate whether a user has paid for a plan before allowing them to send invite links with any role assigned. This could lead to unauthorized access and manipulation of project settings or data.	5.4	More Details
CVE-2024-32713	Missing Authorization vulnerability in AutoWriter AI Post Generator | AutoWriter.This issue affects AI Post Generator | AutoWriter: from n/a through 3.3.	5.4	More Details
CVE-2024-3402	A stored Cross-Site Scripting (XSS) vulnerability existed in version (20240121) of gaizhenbiao/chuanhuchatgpt due to inadequate sanitization and validation of model output data. Despite user-input validation efforts, the application fails to properly sanitize or validate the output from the model, allowing for the injection and execution of malicious JavaScript code within the context of a user's browser. This vulnerability can lead to the execution of arbitrary JavaScript code in the context of other users' browsers, potentially resulting in the hijacking of victims' browsers.	5.4	More Details
CVE-2024-3099	A vulnerability in mlflow/mlflow version 2.11.1 allows attackers to create multiple models with the same name by exploiting URL encoding. This flaw can lead to Denial of Service (DoS) as an authenticated user might not be able to use the intended model, as it will open a different model each time. Additionally, an attacker can exploit this vulnerability to perform data model poisoning by creating a model with the same name, potentially causing an authenticated user to become a victim by using the poisoned model. The issue stems from inadequate validation of model names, allowing for the creation of models with URL-encoded names that are treated as distinct from their URL-decoded counterparts.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36359	A cross-site scripting (XSS) vulnerability in Trend Micro InterScan Web Security Virtual Appliance (IWSVA) 6.5 could allow an attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	5.4	More Details
CVE-2023-23640	Missing Authorization vulnerability in MainWP MainWP UpdraftPlus Extension.This issue affects MainWP UpdraftPlus Extension: from n/a through 4.0.6.	5.4	More Details
CVE-2024-32824	Missing Authorization vulnerability in Evergreen Content Poster.This issue affects Evergreen Content Poster: from n/a through 1.4.2.	5.4	More Details
CVE-2024-34690	SAP Student Life Cycle Management (SLcM) fails to conduct proper authorization checks for authenticated users, leading to the potential escalation of privileges. On successful exploitation it could allow an attacker to access and edit non-sensitive report variants that are typically restricted, causing minimal impact on the confidentiality and integrity of the application.	5.4	More Details
CVE-2024-32797	Missing Authorization vulnerability in Martin Gibson WP LinkedIn Auto Publish.This issue affects WP LinkedIn Auto Publish: from n/a through 8.11.	5.4	More Details
CVE-2024-31403	Incorrect authorization vulnerability in Cybozu Garoon 5.0.0 to 6.0.0 allows a remote authenticated attacker to alter and/or obtain the data of Memo.	5.4	More Details
CVE-2024-35689	Cross-Site Request Forgery (CSRF) vulnerability in Analytify.This issue affects Analytify: from n/a through 5.2.3.	5.4	More Details
CVE-2024-35657	Cross-Site Request Forgery (CSRF) vulnerability in Plechev Andrey WP-Recall.This issue affects WP-Recall: from n/a through 16.26.6.	5.4	More Details
CVE-2024-24704	Missing Authorization vulnerability in AddonMaster Load More Anything.This issue affects Load More Anything: from n/a through 3.3.3.	5.4	More Details
CVE-2024-32144	Missing Authorization vulnerability in Welcart Inc. Welcart e-Commerce.This issue affects Welcart e-Commerce: from n/a through 2.9.14.	5.4	More Details
CVE-2023-52179	Missing Authorization vulnerability in WebCodingPlace Product Expiry for WooCommerce.This issue affects Product Expiry for WooCommerce: from n/a through 2.5.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35663	Missing Authorization vulnerability in HahnCreativeGroup WP Translate.This issue affects WP Translate: from n/a through 5.3.0.	5.4	More Details
CVE-2024-31246	Missing Authorization vulnerability in Post Grid Team by WPXPO PostX – Gutenberg Blocks for Post Grid.This issue affects PostX – Gutenberg Blocks for Post Grid: from n/a through 3.2.3.	5.4	More Details
CVE-2024-30466	Missing Authorization vulnerability in OnTheGoSystems WooCommerce Multilingual & Multicurrency.This issue affects WooCommerce Multilingual & Multicurrency: from n/a through 5.3.4.	5.4	More Details
CVE-2023-52183	Missing Authorization vulnerability in WebToffee WordPress Backup & Migration.This issue affects WordPress Backup & Migration: from n/a through 1.4.3.	5.4	More Details
CVE-2024-30464	Missing Authorization vulnerability in WPZOOM Social Icons Widget & Block by WPZOOM.This issue affects Social Icons Widget & Block by WPZOOM: from n/a through 4.2.15.	5.4	More Details
CVE-2024-24716	Missing Authorization vulnerability in Awesome Support Team Awesome Support.This issue affects Awesome Support: from n/a through 6.1.6.	5.4	More Details
CVE-2024-34804	Missing Authorization vulnerability in Tagembed.This issue affects Tagembed: from n/a through 5.8.	5.4	More Details
CVE-2023-23639	Missing Authorization vulnerability in MainWP MainWP Staging Extension.This issue affects MainWP Staging Extension: from n/a through 4.0.3.	5.4	More Details
CVE-2024-3987	The WP Mobile Menu – The Mobile-Friendly Responsive Menu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via image alt text in all versions up to, and including, 2.8.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2024-5003	The WP Stacker WordPress plugin through 1.8.5 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	5.4	More Details
CVE-2024-36406	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, unchecked input allows for open re-direct. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5607	The GDPR CCPA Compliance & Cookie Consent Banner plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several functions named ajaxUpdateSettings() in all versions up to, and including, 2.7.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify the plugin's settings, update page content, send arbitrary emails and inject malicious web scripts.	5.4	More Details
CVE-2024-3850	Uniview NVR301-04S2-P4 is vulnerable to reflected cross-site scripting attack (XSS). An attacker could send a user a URL that if clicked on could execute malicious JavaScript in their browser. This vulnerability also requires authentication before it can be exploited, so the scope and severity is limited. Also, even if JavaScript is executed, no additional benefits are obtained.	5.4	More Details
CVE-2024-3288	The Logo Slider WordPress plugin before 4.0.0 does not validate and escape some of its Slider Settings before outputting them back in attributes, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-45176	An issue was discovered in LIVEBOX Collaboration vDesk through v018. Stored Cross-site Scripting (XSS) can occur under the /api/v1/getbodyfile endpoint via the uri parameter. The web application (through its vShare functionality section) doesn't properly check parameters, sent in HTTP requests as input, before saving them on the server. In addition, crafted JavaScript content can then be reflected back to the end user and executed by the web browser.	5.4	More Details
CVE-2024-4756	The WP Backpack 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)	5.4	More Details
CVE-2023-6876	The Clever Fox – One Click Website Importer by Nayra Themes plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'clever-fox-activate-theme' function in all versions up to, and including, 25.2.0. This makes it possible for authenticated attackers, with subscriber access and above, to modify the active theme, including to an invalid value which can take down the site.	5.4	More Details
CVE-2024-36775	A cross-site scripting (XSS) vulnerability in Monstra CMS v3.0.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the About Me parameter in the Edit Profile page.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5550	In h2oai/h2o-3 version 3.40.0.4, an exposure of sensitive information vulnerability exists due to an arbitrary system path lookup feature. This vulnerability allows any remote user to view full paths in the entire file system where h2o-3 is hosted. Specifically, the issue resides in the Typeahead API call, which when requested with a typeahead lookup of '/', exposes the root filesystem including directories such as /home, /usr, /bin, among others. This vulnerability could allow attackers to explore the entire filesystem, and when combined with a Local File Inclusion (LFI) vulnerability, could make exploitation of the server trivial.	5.3	More Details
CVE-2024-37296	The Aimeos HTML client provides Aimeos HTML components for e-commerce projects. Starting in version 2020.04.1 and prior to versions 2020.10.27, 2021.10.21, 2022.10.12, 2023.10.14, and 2024.04.5, digital downloads sold in online shops can be downloaded without valid payment, e.g. if the payment didn't succeed. Versions 2020.10.27, 2021.10.21, 2022.10.12, 2023.10.14, and 2024.04.5 fix this issue.	5.3	More Details
CVE-2024-35735	Missing Authorization vulnerability in CodePeople WP Time Slots Booking Form.This issue affects WP Time Slots Booking Form: from n/a through 1.2.11.	5.3	More Details
CVE-2024-35710	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Podlove Podlove Web Player.This issue affects Podlove Web Player: from n/a through 5.7.3.	5.3	More Details
CVE-2024-32811	Insertion of Sensitive Information into Log File vulnerability in Octolize USPS Shipping for WooCommerce – Live Rates.This issue affects USPS Shipping for WooCommerce – Live Rates: from n/a through 1.9.4.	5.3	More Details
CVE-2024-35685	Missing Authorization vulnerability in Anders Norén Radcliffe 2.This issue affects Radcliffe 2: from n/a through 2.0.17.	5.3	More Details
CVE-2024-32813	Missing Authorization vulnerability in SoftLab Integrate Google Drive.This issue affects Integrate Google Drive: from n/a through 1.3.9.	5.3	More Details
CVE-2024-32814	Missing Authorization vulnerability in Zorem Advanced Local Pickup for WooCommerce.This issue affects Advanced Local Pickup for WooCommerce: from n/a through 1.6.1.	5.3	More Details
CVE-2024-2473	The WPS Hide Login plugin for WordPress is vulnerable to Login Page Disclosure in all versions up to, and including, 1.9.15.2. This is due to a bypass that is created when the 'action=postpass' parameter is supplied. This makes it possible for attackers to easily discover any login page that may have been hidden by the plugin.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28164	SAP NetWeaver AS Java (CAF - Guided Procedures) allows an unauthenticated user to access non-sensitive information about the server which would otherwise be restricted causing low impact on confidentiality of the application.	5.3	More Details
CVE-2024-35683	Missing Authorization vulnerability in Teplitsa of social technologies Leyka.This issue affects Leyka: from n/a through 3.31.1.	5.3	More Details
CVE-2024-32820	Missing Authorization vulnerability in Social Share Pro Social Share Icons & Social Share Buttons.This issue affects Social Share Icons & Social Share Buttons: from n/a through 3.6.2.	5.3	More Details
CVE-2023-51498	Missing Authorization vulnerability in Woo WooCommerce Canada Post Shipping.This issue affects WooCommerce Canada Post Shipping: from n/a through 2.8.3.	5.3	More Details
CVE-2024-22151	Missing Authorization vulnerability in Codection Import and export users and customers.This issue affects Import and export users and customers: from n/a through 1.24.6.	5.3	More Details
CVE-2024-34406	Improper exception handling in McAfee Security: Antivirus VPN for Android before 8.3.0 could allow an attacker to cause a denial of service through the use of a malformed deep link.	5.3	More Details
CVE-2024-32727	Missing Authorization vulnerability in Rometheme RomethemeForm For Elementor.This issue affects RomethemeForm For Elementor: from n/a through 1.1.2.	5.3	More Details
CVE-2024-33545	Missing Authorization vulnerability in AA-Team WZone.This issue affects WZone: from n/a through 14.0.10.	5.3	More Details
CVE-2024-31878	IBM i 7.2, 7.3, 7.4, and 7.5 Service Tools Server (SST) is vulnerable to SST user enumeration by a remote attacker. This vulnerability can be used by a malicious actor to gather information about SST users that can be targeted in further attacks. IBM X-Force ID: 287538.	5.3	More Details
CVE-2024-37152	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. The vulnerability allows unauthorized access to the sensitive settings exposed by /api/v1/settings endpoint without authentication. All sensitive settings are hidden except passwordPattern. This vulnerability is fixed in 2.11.3, 2.10.12, and 2.9.17.	5.3	More Details
CVE-2024-32799	Missing Authorization vulnerability in Merv Barrett Easy Property Listings.This issue affects Easy Property Listings: from n/a through 3.5.3.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1689	The WooCommerce Tools plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the woocommerce_tool_toggle_module() function in all versions up to, and including, 1.2.9. This makes it possible for authenticated attackers, with subscriber-level access and above, to deactivate arbitrary plugin modules.	5.3	More Details
CVE-2024-32715	Missing Authorization vulnerability in Olive Themes Olive One Click Demo Import.This issue affects Olive One Click Demo Import: from n/a through 1.1.1.	5.3	More Details
CVE-2024-3723	The Advanced Contact form 7 DB plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.0.2 via the wp-content/uploads/advanced-cf7-upload directory. This makes it possible for unauthenticated attackers to extract sensitive data uploaded via this plugin through a form.	5.3	More Details
CVE-2024-34821	Missing Authorization vulnerability in Contact List PRO Contact List – Easy Business Directory, Staff Directory and Address Book Plugin.This issue affects Contact List – Easy Business Directory, Staff Directory and Address Book Plugin: from n/a through 2.9.87.	5.3	More Details
CVE-2023-52186	Missing Authorization vulnerability in Woo WooCommerce Product Vendors.This issue affects WooCommerce Product Vendors: from n/a through 2.2.2.	5.3	More Details
CVE-2024-34822	Missing Authorization vulnerability in weDevs weMail.This issue affects weMail: from n/a through 1.14.2.	5.3	More Details
CVE-2023-28775	Missing Authorization vulnerability in Yoast Yoast SEO Premium.This issue affects Yoast SEO Premium: from n/a through 20.4.	5.3	More Details
CVE-2024-35659	Authorization Bypass Through User-Controlled Key vulnerability in KiviCare.This issue affects KiviCare: from n/a through 3.6.2.	5.3	More Details
CVE-2023-48273	Missing Authorization vulnerability in WP OnlineSupport, Essential Plugin Preloader for Website.This issue affects Preloader for Website: from n/a through 1.2.2.	5.3	More Details
CVE-2024-4266	The MetForm – Contact Form, Survey, Quiz, & Custom Form Builder for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 3.8.8 via the 'handle_file' function. This can allow unauthenticated attackers to extract sensitive data, such as Personally Identifiable Information, from files uploaded by users.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4319	The Advanced Contact form 7 DB plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'vsz_cf7_export_to_excel' function in versions up to, and including, 2.0.2. This makes it possible for unauthenticated attackers to download the entry data for submitted forms.	5.3	More Details
CVE-2024-35692	Missing Authorization vulnerability in Termly Cookie Consent.This issue affects Cookie Consent: from n/a through 3.2.	5.3	More Details
CVE-2024-34813	Missing Authorization vulnerability in MoreConvert MC Woocommerce Wishlist.This issue affects MC Woocommerce Wishlist: from n/a through 1.7.8.	5.3	More Details
CVE-2024-32779	Missing Authorization vulnerability in Avirtum Vision Interactive.This issue affects Vision Interactive: from n/a through 1.7.1.	5.3	More Details
CVE-2024-34753	Missing Authorization vulnerability in SoftLab Radio Player.This issue affects Radio Player: from n/a through 2.0.73.	5.3	More Details
CVE-2024-35728	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Themeisle PPOM for WooCommerce allows Code Inclusion.This issue affects PPOM for WooCommerce: from n/a through 32.0.20.	5.3	More Details
CVE-2024-35729	Missing Authorization vulnerability in Tickera.This issue affects Tickera: from n/a through 3.5.2.6.	5.3	More Details
CVE-2024-5483	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.2.6.8 due to incorrect implementation of get_items_permissions_check function. This makes it possible for unauthenticated attackers to extract basic information about website users, including their emails	5.3	More Details
CVE-2024-35747	Improper Restriction of Excessive Authentication Attempts vulnerability in wpdevart Contact Form Builder, Contact Widget allows Functionality Bypass.This issue affects Contact Form Builder, Contact Widget: from n/a through 2.1.7.	5.3	More Details
CVE-2024-23521	Missing Authorization vulnerability in Happyforms.This issue affects Happyforms: from n/a through 1.25.10.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51682	Missing Authorization vulnerability in ibericode MC4WP.This issue affects MC4WP: from n/a through 4.9.9.	5.3	More Details
CVE-2024-37168	@grpc/grps-js implements the core functionality of gRPC purely in JavaScript, without a C++ addon. Prior to versions 1.10.9, 1.9.15, and 1.8.22, there are two separate code paths in which memory can be allocated per message in excess of the `grpc.max_receive_message_length` channel option: If an incoming message has a size on the wire greater than the configured limit, the entire message is buffered before it is discarded; and/or if an incoming message has a size within the limit on the wire but decompresses to a size greater than the limit, the entire message is decompressed into memory, and on the server is not discarded. This has been patched in versions 1.10.9, 1.9.15, and 1.8.22.	5.3	More Details
CVE-2024-37169	@jmondi/url-to-png is a self-hosted URL to PNG utility. Versions prior to 2.0.3 are vulnerable to arbitrary file read if a threat actor uses the Playright's screenshot feature to exploit the file wrapper. Version 2.0.3 mitigates this issue by requiring input URLs to be of protocol `http` or `https`. No known workarounds are available aside from upgrading.	5.3	More Details
CVE-2024-36473	Trend Micro VPN Proxy One Pro, version 5.8.1012 and below is vulnerable to an arbitrary file overwrite or create attack but is limited to local Denial of Service (DoS) and under specific conditions can lead to elevation of privileges.	5.3	More Details
CVE-2024-30538	Missing Authorization vulnerability in DELUCKS GmbH DELUCKS SEO.This issue affects DELUCKS SEO: from n/a through 2.5.4.	5.3	More Details
CVE-2024-34819	Missing Authorization vulnerability in MoreConvert MC Woocommerce Wishlist.This issue affects MC Woocommerce Wishlist: from n/a through 1.7.2.	5.3	More Details
CVE-2024-34758	Missing Authorization vulnerability in Wpmet WP Fundraising Donation and Crowdfunding Platform.This issue affects WP Fundraising Donation and Crowdfunding Platform: from n/a through 1.6.4.	5.3	More Details
CVE-2024-34763	Missing Authorization vulnerability in Tobias Conrad Builder for WooCommerce reviews shortcodes – ReviewShort.This issue affects Builder for WooCommerce reviews shortcodes – ReviewShort: from n/a through 1.01.5.	5.3	More Details
CVE-2024-34802	Missing Authorization vulnerability in AdFoxly AdFoxly – Ad Manager, AdSense Ads & Ads.Txt.This issue affects AdFoxly – Ad Manager, AdSense Ads & Ads.Txt: from n/a through 1.8.5.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35661	Missing Authorization vulnerability in SoftLab Upload Fields for WPForms.This issue affects Upload Fields for WPForms: from n/a through 1.0.2.	5.3	More Details
CVE-2024-0972	The BuddyPress Members Only plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.3.5 via the REST API. This makes it possible for unauthenticated attackers to bypass the plugin's "All Other Sections On Your Site Will be Opened to Guest" feature (when unset) and view restricted page and post content.	5.3	More Details
CVE-2024-1175	The WP-Recall – Registration, Profile, Commerce & More plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'delete_payment' function in all versions up to, and including, 16.26.6. This makes it possible for unauthenticated attackers to delete arbitrary payments.	5.3	More Details
CVE-2024-35742	Missing Authorization vulnerability in Code Parrots Easy Forms for Mailchimp.This issue affects Easy Forms for Mailchimp: from n/a through 6.9.0.	5.3	More Details
CVE-2024-35748	Missing Authorization vulnerability in OPMC WooCommerce Dropshipping.This issue affects WooCommerce Dropshipping: from n/a through 5.0.4.	5.3	More Details
CVE-2024-5458	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.	5.3	More Details
CVE-2024-30539	Missing Authorization vulnerability in Awesome Support Team Awesome Support.This issue affects Awesome Support: from n/a through 6.1.7.	5.3	More Details
CVE-2024-34768	Missing Authorization vulnerability in Fastly.This issue affects Fastly: from n/a through 1.2.25.	5.3	More Details
CVE-2024-22298	Missing Authorization vulnerability in TMS Amelia ameliabooking.This issue affects Amelia: from n/a through 1.0.98.	5.3	More Details
CVE-2024-23524	Missing Authorization vulnerability in ONTRAPORT Inc. PilotPress.This issue affects PilotPress: from n/a through 2.0.30.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5615	The Open Graph plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.11.2 via the 'opengraph_default_description' function. This makes it possible for unauthenticated attackers to extract sensitive data including partial content of password-protected blog posts.	5.3	More Details
CVE-2024-1272	Inclusion of Sensitive Information in Source Code vulnerability in TNB Mobile Solutions Cockpit Software allows Retrieve Embedded Sensitive Data.This issue affects Cockpit Software: before v0.251.1.	5.3	More Details
CVE-2023-49927	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, Exynos 990, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 9110, Exynos W920, Exynos Modem 5123, Exynos Modem 5300. The baseband software does not properly check format types specified by the RRC. This can lead to a lack of encryption.	5.3	More Details
CVE-2024-31276	Missing Authorization vulnerability in WPFactory Products, Order & Customers Export for WooCommerce.This issue affects Products, Order & Customers Export for WooCommerce: from n/a through 2.0.8.	5.3	More Details
CVE-2024-4744	Missing Authorization vulnerability in Avirtum iPages Flipbook.This issue affects iPages Flipbook: from n/a through 1.5.1.	5.3	More Details
CVE-2024-34442	Missing Authorization vulnerability in weDevs weDocs.This issue affects weDocs: from n/a through 2.1.4.	5.3	More Details
CVE-2024-0910	The Restrict for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.6 due to improper restrictions on hidden data that make it accessible through the REST API. This makes it possible for unauthenticated attackers to extract potentially sensitive data from post content.	5.3	More Details
CVE-2024-31274	Missing Authorization vulnerability in WPDeveloper EmbedPress.This issue affects EmbedPress: from n/a through 3.9.11.	5.3	More Details
CVE-2024-31273	Missing Authorization vulnerability in JS Help Desk JS Help Desk – Best Help Desk & Support Plugin.This issue affects JS Help Desk – Best Help Desk & Support Plugin: from n/a through 2.8.3.	5.3	More Details
CVE-2024-32725	Missing Authorization vulnerability in Saleswonder 5 Stars Rating Funnel.This issue affects 5 Stars Rating Funnel: from n/a through 1.2.67.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35667	Missing Authorization vulnerability in WP EasyCart.This issue affects WP EasyCart: from n/a through 5.5.19.	5.3	More Details
CVE-2024-35665	Missing Authorization vulnerability in namithjawahar Insert Post Ads.This issue affects Insert Post Ads: from n/a through 1.3.2.	5.3	More Details
CVE-2024-35680	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in YITH YITH WooCommerce Product Add-Ons allows Code Injection.This issue affects YITH WooCommerce Product Add-Ons: from n/a through 4.9.2.	5.3	More Details
CVE-2024-30529	Missing Authorization vulnerability in Tainacan.Org Tainacan.This issue affects Tainacan: from n/a through 0.20.7.	5.3	More Details
CVE-2023-51494	Missing Authorization vulnerability in Woo WooCommerce Product Vendors.This issue affects WooCommerce Product Vendors: from n/a through 2.2.1.	5.3	More Details
CVE-2024-36735	OneFlow-Inc. Oneflow v0.9.1 does not display an error or warning when the oneflow.eye parameter is floating.	5.3	More Details
CVE-2024-31352	Missing Authorization vulnerability in Email Subscribers & Newsletters.This issue affects Email Subscribers & Newsletters: from n/a through 5.7.13.	5.3	More Details
CVE-2024-37154	Evmos is the Ethereum Virtual Machine (EVM) Hub on the Cosmos Network. Users are able to delegate tokens that have not yet been vested. This affects employees and grantees who have funds managed via `ClawbackVestingAccount`. This affects 18.1.0 and earlier.	5.3	More Details
CVE-2022-32933	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Monterey 12.5. A website may be able to track the websites a user visited in Safari private browsing mode.	5.3	More Details
CVE-2024-3102	A JSON Injection vulnerability exists in the `mintplex-labs/anything-llm` application, specifically within the username parameter during the login process at the `/api/request-token` endpoint. The vulnerability arises from improper handling of values, allowing attackers to perform brute force attacks without prior knowledge of the username. Once the password is known, attackers can conduct blind attacks to ascertain the full username, significantly compromising system security.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5687	If a specific sequence of actions is performed when opening a new tab, the triggering principal associated with the new tab may have been incorrect. The triggering principal is used to calculate many values, including the `Referer` and `Sec-*` headers, meaning there is the potential for incorrect security checks within the browser in addition to incorrect or misleading information sent to remote websites. *This bug only affects Firefox for Android. Other versions of Firefox are unaffected.* This vulnerability affects Firefox < 127.	5.3	More Details
CVE-2024-30544	Missing Authorization vulnerability in UPQODE Whizzy.This issue affects Whizzy: from n/a through 1.1.18.	5.3	More Details
CVE-2024-22326	IBM System Storage DS8900F 89.22.19.0, 89.30.68.0, 89.32.40.0, 89.33.48.0, 89.40.83.0, and 89.40.93.0 could allow a remote user to create an LDAP connection with a valid username and empty password to establish an anonymous connection. IBM X-Force ID: 279518.	5.0	More Details
CVE-2024-37178	SAP Financial Consolidation does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. These endpoints are exposed over the network. The vulnerability can exploit resources beyond the vulnerable component. On successful exploitation, an attacker can cause limited impact to confidentiality of the application.	5.0	More Details
CVE-2024-31397	Improper handling of extra values issue exists in Cybozu Garoon 5.0.0 to 5.15.2. If this vulnerability is exploited, a user who can log in to the product with the administrative privilege may be able to cause a denial-of-service (DoS) condition.	4.9	More Details
CVE-2023-50763	A vulnerability has been identified in SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0) (All versions < V2.3), SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0) (All versions < V2.3), SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0) (All versions < V2.3), SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) (All versions < V2.4.8), TIM 1531 IRC (6GK7543-1MX00-0XE0) (All versions < V2.4.8). The web server of affected products, if configured to allow the import of PKCS12 containers, could end up in an infinite loop when processing incomplete certificate chains. This could allow an authenticated remote attacker to create a denial of service condition by importing specially crafted PKCS12 containers.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35712	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Jordy Meow Database Cleaner allows Relative Path Traversal.This issue affects Database Cleaner: from n/a through 1.0.5.	4.9	More Details
CVE-2024-35650	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Melapress MelaPress Login Security allows PHP Remote File Inclusion.This issue affects MelaPress Login Security: from n/a through 1.3.0.	4.9	More Details
CVE-2024-4890	A blind SQL injection vulnerability exists in the berriai/litellm application, specifically within the '/team/update' process. The vulnerability arises due to the improper handling of the 'user_id' parameter in the raw SQL query used for deleting users. An attacker can exploit this vulnerability by injecting malicious SQL commands through the 'user_id' parameter, leading to potential unauthorized access to sensitive information such as API keys, user information, and tokens stored in the database. The affected version is 1.27.14.	4.9	More Details
CVE-2024-2171	A stored Cross-Site Scripting (XSS) vulnerability was identified in the zenml-io/zenml repository, specifically within the 'logo_url' field. By injecting malicious payloads into this field, an attacker could send harmful messages to other users, potentially compromising their accounts. The vulnerability affects version 0.55.3 and was fixed in version 0.56.2. The impact of exploiting this vulnerability could lead to user account compromise.	4.8	More Details
CVE-2024-5658	The CraftCMS plugin Two-Factor Authentication through 3.3.3 allows reuse of TOTP tokens multiple times within the validity period.	4.8	More Details
CVE-2024-4812	A flaw was found in the Katello plugin for Foreman, where it is possible to store malicious JavaScript code in the "Description" field of a user. This code can be executed when opening certain pages, for example, Host Collections.	4.8	More Details
CVE-2024-37160	Formwork is a flat file-based Content Management System (CMS). An attackers (requires administrator privilege) to execute arbitrary web scripts by modifying site options via /panel/options/site. This type of attack is suitable for persistence, affecting visitors across all pages (except the dashboard). This vulnerability is fixed in 1.13.1.	4.8	More Details
CVE-2024-36773	A cross-site scripting (XSS) vulnerability in Monstra CMS v3.0.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Themes parameter at index.php.	4.8	More Details
CVE-2024-36788	Netgear WNR614 JNR1010V2 N300-V1.1.0.54_1.0.1 does not properly set the HTTPOnly flag for cookies. This allows attackers to possibly intercept and access sensitive communications between the router and connected devices.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4621	The ARForms - Premium WordPress Form Builder Plugin WordPress plugin before 6.6 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-2024-20405	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct a stored XSS attack by exploiting an RFI vulnerability. This vulnerability is due to insufficient validation of user-supplied input for specific HTTP requests that are sent to an affected device. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive information on the affected device.	4.8	More Details
CVE-2023-5424	The WS Form LITE plugin for WordPress is vulnerable to CSV Injection in versions up to, and including, 1.9.217. This allows unauthenticated attackers to embed untrusted input into exported CSV files, which can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration.	4.7	More Details
CVE-2024-36307	A security agent link following vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to disclose sensitive information about the agent on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	4.7	More Details
CVE-2024-30052	Visual Studio Remote Code Execution Vulnerability	4.7	More Details
CVE-2024-2965	A Denial-of-Service (DoS) vulnerability exists in the `SitemapLoader` class of the `langchain-ai/langchain` repository, affecting all versions. The `parse_sitemap` method, responsible for parsing sitemaps and extracting URLs, lacks a mechanism to prevent infinite recursion when a sitemap URL refers to the current sitemap itself. This oversight allows for the possibility of an infinite loop, leading to a crash by exceeding the maximum recursion depth in Python. This vulnerability can be exploited to occupy server socket/port resources and crash the Python process, impacting the availability of services relying on this functionality.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5206	A sensitive data leakage vulnerability was identified in scikit-learn's TfidfVectorizer, specifically in versions up to and including 1.4.1.post1, which was fixed in version 1.5.0. The vulnerability arises from the unexpected storage of all tokens present in the training data within the `stop_words_` attribute, rather than only storing the subset of tokens required for the TF-IDF technique to function. This behavior leads to the potential leakage of sensitive information, as the `stop_words_` attribute could contain tokens that were meant to be discarded and not stored, such as passwords or keys. The impact of this vulnerability varies based on the nature of the data being processed by the vectorizer.	4.7	More Details
CVE-2024-30069	Windows Remote Access Connection Manager Information Disclosure Vulnerability	4.7	More Details
CVE-2024-5691	By tricking the browser with a `X-Frame-Options` header, a sandboxed iframe could have presented a button that, if clicked by a user, would bypass restrictions to open a new window. This vulnerability affects Firefox < 127, Firefox ESR < 115.12, and Thunderbird < 115.12.	4.7	More Details
CVE-2024-5629	An out-of-bounds read in the 'bson' module of PyMongo 4.6.2 or earlier allows deserialization of malformed BSON provided by a Server to raise an exception which may contain arbitrary application memory.	4.7	More Details
CVE-2024-23251	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.5, watchOS 10.5, iOS 17.5 and iPadOS 17.5, iOS 16.7.8 and iPadOS 16.7.8. An attacker with physical access may be able to leak Mail account credentials.	4.6	More Details
CVE-2024-35253	Microsoft Azure File Sync Elevation of Privilege Vulnerability	4.4	More Details
CVE-2024-4942	The Custom Dash plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35235	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. In versions 2.4.8 and earlier, when starting the cupsd server with a Listen configuration item pointing to a symbolic link, the cupsd process can be caused to perform an arbitrary chmod of the provided argument, providing world-writable access to the target. Given that cupsd is often running as root, this can result in the change of permission of any user or system files to be world writable. Given the aforementioned Ubuntu AppArmor context, on such systems this vulnerability is limited to those files modifiable by the cupsd process. In that specific case it was found to be possible to turn the configuration of the Listen argument into full control over the cupsd.conf and cups-files.conf configuration files. By later setting the User and Group arguments in cups-files.conf, and printing with a printer configured by PPD with a `FoomaticRIPCommandLine` argument, arbitrary user and group (not root) command execution could be achieved, which can further be used on Ubuntu systems to achieve full root command execution. Commit ff1f8a623e090dee8a8aadf12a6a4b25efac143d contains a patch for the issue.	4.4	More Details
CVE-2024-37535	GNOME VTE before 0.76.3 allows an attacker to cause a denial of service (memory consumption) via a window resize escape sequence, a related issue to CVE-2000-0476.	4.4	More Details
CVE-2023-45707	HCL Connections Docs is vulnerable to a cross-site scripting attack where an attacker may leverage this issue to execute arbitrary code. This may lead to credentials disclosure and possibly launch additional attacks.	4.4	More Details
CVE-2024-0653	The Custom Field Template plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.6.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-4468	The Salon booking system plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on several functions hooked into admin_init in all versions up to, and including, 9.9. This makes it possible for authenticated attackers with subscriber access or higher to modify plugin settings and view discount codes intended for other users.	4.3	More Details
CVE-2024-32146	Missing Authorization vulnerability in Aspose.Cloud Marketplace Aspose.Words Exporter.This issue affects Aspose.Words Exporter: from n/a through 6.3.1.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23518	Missing Authorization vulnerability in Navneil Naicker ACF Photo Gallery Field.This issue affects ACF Photo Gallery Field: from n/a through 2.6.	4.3	More Details
CVE-2024-5438	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.7.1 via the 'attempt_delete' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Instructor-level access and above, to delete arbitrary quiz attempts.	4.3	More Details
CVE-2024-23503	Missing Authorization vulnerability in WPManageNinja LLC Ninja Tables.This issue affects Ninja Tables: from n/a through 5.0.6.	4.3	More Details
CVE-2024-35674	Missing Authorization vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates).This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 1.5.109.	4.3	More Details
CVE-2024-35684	Cross-Site Request Forgery (CSRF) vulnerability in 10up ElasticPress.This issue affects ElasticPress: from n/a through 5.1.1.	4.3	More Details
CVE-2023-51519	Missing Authorization vulnerability in Soliloquy Team Slider by Soliloquy.This issue affects Slider by Soliloquy: from n/a through 2.7.2.	4.3	More Details
CVE-2024-35682	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Themeisle Otter Blocks PRO.This issue affects Otter Blocks PRO: from n/a through 2.6.11.	4.3	More Details
CVE-2024-31294	Missing Authorization vulnerability in Fahad Mahmood WP Sort Order.This issue affects WP Sort Order: from n/a through 1.3.1.	4.3	More Details
CVE-2024-5453	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the pm_dismissible_notice and pm_wizard_update_group_icon functions in all versions up to, and including, 5.8.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change arbitrary options to the value '1' or change group icons.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4088	The Gutenberg Blocks and Page Layouts – Attire Blocks plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the disable_fe_assets function in all versions up to, and including, 1.9.2. This makes it possible for authenticated attackers, with subscriber access or above, to change the plugin's settings. Additionally, no nonce check is performed resulting in a CSRF vulnerability.	4.3	More Details
CVE-2024-2368	The Mollie Forms plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.6.13. This is due to missing or incorrect nonce validation on the duplicateForm() function. This makes it possible for unauthenticated attackers to duplicate forms via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-31495	A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiPortal versions 7.0.0 through 7.0.6 and version 7.2.0 allows privileged user to obtain unauthorized information via the report download functionality.	4.3	More Details
CVE-2024-4886	The contains an IDOR vulnerability that allows a user to comment on a private post by manipulating the ID included in the request	4.3	More Details
CVE-2024-32143	Missing Authorization vulnerability in Podlove Podlove Podcast Publisher.This issue affects Podlove Podcast Publisher: from n/a through 4.1.0.	4.3	More Details
CVE-2024-32148	Missing Authorization vulnerability in Salesforce Pardot.This issue affects Pardot: from n/a through 2.1.0.	4.3	More Details
CVE-2024-30537	Missing Authorization vulnerability in WPClever WPC Badge Management for WooCommerce.This issue affects WPC Badge Management for WooCommerce: from n/a through 2.4.0.	4.3	More Details
CVE-2024-21748	Missing Authorization vulnerability in Icegram.This issue affects Icegram: from n/a through 3.1.21.	4.3	More Details
CVE-2023-6491	The Strong Testimonials plugin for WordPress is vulnerable to unauthorized modification of data due to an improper capability check on the wpmtst_save_view_sticky function in all versions up to, and including, 3.1.12. This makes it possible for authenticated attackers, with contributor access and above, to modify favorite views.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4661	The WP Reset plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_ajax function in all versions up to, and including, 2.02. This makes it possible for authenticated attackers, with subscriber-level access and above, to modify the value fo the 'License Key' field for the 'Activate Pro License' setting.	4.3	More Details
CVE-2024-35168	Missing Authorization vulnerability in Discourse WP Discourse.This issue affects WP Discourse: from n/a through 2.5.1.	4.3	More Details
CVE-2023-52227	Missing Authorization vulnerability in MailerLite MailerLite – WooCommerce integration.This issue affects MailerLite – WooCommerce integration: from n/a through 2.0.8.	4.3	More Details
CVE-2024-35628	Missing Authorization vulnerability in Photo Gallery Team Photo Gallery by 10Web.This issue affects Photo Gallery by 10Web: from n/a through 1.8.25.	4.3	More Details
CVE-2024-5459	The Restaurant Menu and Food Ordering plugin for WordPress is vulnerable to unauthorized creation of data due to a missing capability check on 'add_section', 'add_menu', 'add_menu_item', and 'add_menu_page' functions in all versions up to, and including, 2.4.16. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create menu sections, menus, food items, and new menu pages.	4.3	More Details
CVE-2024-35673	Cross-Site Request Forgery (CSRF) vulnerability in Pure Chat by Ruby Pure Chat.This issue affects Pure Chat: from n/a through 2.22.	4.3	More Details
CVE-2023-52224	Missing Authorization vulnerability in Revolut Revolut Gateway for WooCommerce.This issue affects Revolut Gateway for WooCommerce: from n/a through 4.9.7.	4.3	More Details
CVE-2024-31248	Missing Authorization vulnerability in Team Plugins360 All-in-One Video Gallery.This issue affects All-in-One Video Gallery: from n/a through 3.5.2.	4.3	More Details
CVE-2024-32804	Missing Authorization vulnerability in Martin Gibson WP GoToWebinar.This issue affects WP GoToWebinar: from n/a through 14.46.	4.3	More Details
CVE-2024-32821	Missing Authorization vulnerability in TotalSuite Total Poll Lite.This issue affects Total Poll Lite: from n/a through 4.9.9.	4.3	More Details
CVE-2023-33922	Missing Authorization vulnerability in Elementor Elementor Website Builder.This issue affects Elementor Website Builder: from n/a through 3.13.2.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31359	Missing Authorization vulnerability in Premmerce Premmerce Product Filter for WooCommerce.This issue affects Premmerce Product Filter for WooCommerce: from n/a through 3.7.2.	4.3	More Details
CVE-2024-34435	Missing Authorization vulnerability in CodeRevolution Aiomatic.This issue affects Aiomatic: from n/a through 1.9.3.	4.3	More Details
CVE-2024-35669	Missing Authorization vulnerability in Bowo Debug Log Manager.This issue affects Debug Log Manager: from n/a through 2.3.1.	4.3	More Details
CVE-2024-31402	Incorrect authorization vulnerability in Cybozu Garoon 5.0.0 to 5.15.2 allows a remote authenticated attacker to delete the data of Shared To-Dos.	4.3	More Details
CVE-2024-31398	Insertion of sensitive information into sent data issue exists in Cybozu Garoon 5.0.0 to 5.15.2. If this vulnerability is exploited, a user who can log in to the product may obtain information on the list of users.	4.3	More Details
CVE-2024-32783	Missing Authorization vulnerability in wpcreativeidea Advanced Testimonial Carousel for Elementor.This issue affects Advanced Testimonial Carousel for Elementor: from n/a through 3.0.0.	4.3	More Details
CVE-2024-31350	Missing Authorization vulnerability in AWP Classifieds Team AWP Classifieds.This issue affects AWP Classifieds: from n/a through 4.3.1.	4.3	More Details
CVE-2024-31404	Insertion of sensitive information into sent data issue exists in Cybozu Garoon 5.5.0 to 6.0.0, which may allow a user who can log in to the product to view the data of Scheduler.	4.3	More Details
CVE-2024-32784	Missing Authorization vulnerability in CookieHub.This issue affects CookieHub: from n/a through 1.1.0.	4.3	More Details
CVE-2024-31347	Missing Authorization vulnerability in Data443 Tracking Code Manager.This issue affects Tracking Code Manager: from n/a through 2.1.0.	4.3	More Details
CVE-2024-35727	Missing Authorization vulnerability in actpro Extra Product Options for WooCommerce.This issue affects Extra Product Options for WooCommerce: from n/a through 3.0.6.	4.3	More Details
CVE-2024-32787	Missing Authorization vulnerability in Copy Content Protection Team Secure Copy Content Protection and Content Locking.This issue affects Secure Copy Content Protection and Content Locking: from n/a through 3.7.1.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32792	Missing Authorization vulnerability in WPMU DEV Hummingbird.This issue affects Hummingbird: from n/a through 3.7.3.	4.3	More Details
CVE-2024-35722	Missing Authorization vulnerability in A WP Life Slider Responsive Slideshow – Image slider, Gallery slideshow.This issue affects Slider Responsive Slideshow – Image slider, Gallery slideshow: from n/a through 1.4.0.	4.3	More Details
CVE-2024-36419	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. A vulnerability in versions prior to 8.6.1 allows for Host Header Injection when directly accessing the `/legacy` route. Version 8.6.1 contains a patch for the issue.	4.3	More Details
CVE-2024-35671	Missing Authorization vulnerability in Minoji MJ Update History.This issue affects MJ Update History: from n/a through 1.0.4.	4.3	More Details
CVE-2024-32714	Missing Authorization vulnerability in Academy LMS academy.This issue affects Academy LMS: from n/a through 1.9.16.	4.3	More Details
CVE-2024-22244	Open Redirect in Harbor <=v2.8.4, <=v2.9.2, and <=v2.10.0 may redirect a user to a malicious site.	4.3	More Details
CVE-2024-4746	Missing Authorization vulnerability in Netgsm.This issue affects Netgsm: from n/a through 2.9.16.	4.3	More Details
CVE-2024-5665	The Login/Signup Popup (Inline Form + Woocommerce) plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the ‘export_settings’ function in versions 2.7.1 to 2.7.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read arbitrary options on affected sites.	4.3	More Details
CVE-2024-4745	Missing Authorization vulnerability in RafflePress Giveaways and Contests by RafflePress.This issue affects Giveaways and Contests by RafflePress: from n/a through 1.12.4.	4.3	More Details
CVE-2024-35741	Missing Authorization vulnerability in Awesome Support Team Awesome Support.This issue affects Awesome Support: from n/a through 6.1.7.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5449	The WP Dark Mode – WordPress Dark Mode Plugin for Improved Accessibility, Dark Theme, Night Mode, and Social Sharing plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the wpdm_social_share_save_options function in all versions up to, and including, 5.0.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugin's settings.	4.3	More Details
CVE-2024-32818	Missing Authorization vulnerability in realmag777 WordPress Meta Data and Taxonomies Filter (MDTF).This issue affects WordPress Meta Data and Taxonomies Filter (MDTF): from n/a through 1.3.3.	4.3	More Details
CVE-2023-52217	Missing Authorization vulnerability in weDevs WooCommerce Conversion Tracking.This issue affects WooCommerce Conversion Tracking: from n/a through 2.0.11.	4.3	More Details
CVE-2024-34824	Missing Authorization vulnerability in ThemeBoy SportsPress – Sports Club & League Manager.This issue affects SportsPress – Sports Club & League Manager: from n/a through 2.7.20.	4.3	More Details
CVE-2024-33572	Missing Authorization vulnerability in POSIMYTH The Plus Blocks for Block Editor	Gutenberg.This issue affects The Plus Blocks for Block Editor	Gutenberg: from n/a through 3.2.5.	4.3	More Details
CVE-2024-31423	Missing Authorization vulnerability in Alex Volkov WP Accessibility Helper (WAH).This issue affects WP Accessibility Helper (WAH): from n/a through 0.6.2.5.	4.3	More Details
CVE-2024-27807	The issue was addressed with improved checks. This issue is fixed in iOS 17.5 and iPadOS 17.5, iOS 16.7.8 and iPadOS 16.7.8. An app may be able to circumvent App Privacy Report logging.	4.3	More Details
CVE-2024-35723	Missing Authorization vulnerability in Andrew Rapps Dashboard To-Do List.This issue affects Dashboard To-Do List: from n/a through 1.2.0.	4.3	More Details
CVE-2024-35724	Missing Authorization vulnerability in Bosa Themes Bosa Elementor Addons and Templates for WooCommerce.This issue affects Bosa Elementor Addons and Templates for WooCommerce: from n/a through 1.0.12.	4.3	More Details
CVE-2024-5697	A website was able to detect when a user took a screenshot of a page using the built-in Screenshot functionality in Firefox. This vulnerability affects Firefox < 127.	4.3	More Details
CVE-2024-35721	Missing Authorization vulnerability in A WP Life Image Gallery – Lightbox Gallery, Responsive Photo Gallery, Masonry Gallery.This issue affects Image Gallery – Lightbox Gallery, Responsive Photo Gallery, Masonry Gallery: from n/a through 1.4.5.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30515	Missing Authorization vulnerability in Pixelite Events Manager.This issue affects Events Manager: from n/a through 6.4.6.4.	4.3	More Details
CVE-2024-30517	Missing Authorization vulnerability in Sliced Invoices.This issue affects Sliced Invoices: from n/a through 3.9.2.	4.3	More Details
CVE-2024-5690	By monitoring the time certain operations take, an attacker could have guessed which external protocol handlers were functional on a user's system. This vulnerability affects Firefox < 127, Firefox ESR < 115.12, and Thunderbird < 115.12.	4.3	More Details
CVE-2024-5689	In addition to detecting when a user was taking a screenshot (XXX), a website was able to overlay the 'My Shots' button that appeared, and direct the user to a replica Firefox Screenshots page that could be used for phishing. This vulnerability affects Firefox < 127.	4.3	More Details
CVE-2024-35720	Missing Authorization vulnerability in A WP Life Album Gallery – WordPress Gallery.This issue affects Album Gallery – WordPress Gallery: from n/a through 1.5.7.	4.3	More Details
CVE-2024-35717	Missing Authorization vulnerability in A WP Life Media Slider – Photo Sleder, Video Slider, Link Slider, Carousal Slideshow.This issue affects Media Slider – Photo Sleder, Video Slider, Link Slider, Carousal Slideshow: from n/a through 1.3.9.	4.3	More Details
CVE-2024-35725	Missing Authorization vulnerability in LA-Studio LA-Studio Element Kit for Elementor.This issue affects LA-Studio Element Kit for Elementor: from n/a through 1.3.6.	4.3	More Details
CVE-2024-36106	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. It’s possible for authenticated users to enumerate clusters by name by inspecting error messages. It’s also possible to enumerate the names of projects with project-scoped clusters if you know the names of the clusters. This vulnerability is fixed in 2.11.3, 2.10.12, and 2.9.17.	4.3	More Details
CVE-2024-31252	Missing Authorization vulnerability in dFactory Responsive Lightbox.This issue affects Responsive Lightbox: from n/a through 2.4.6.	4.3	More Details
CVE-2024-31261	Missing Authorization vulnerability in Aakash Chakravarthy Announcer – Notification & message bars.This issue affects Announcer – Notification & message bars: from n/a through 6.0.	4.3	More Details
CVE-2024-31267	Missing Authorization vulnerability in WP Desk Flexible Checkout Fields for WooCommerce.This issue affects Flexible Checkout Fields for WooCommerce: from n/a through 4.1.2.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35726	Missing Authorization vulnerability in ThemeKraft WooBuddy.This issue affects WooBuddy: from n/a through 3.4.19.	4.3	More Details
CVE-2024-22296	Missing Authorization vulnerability in Code for Recovery 12 Step Meeting List.This issue affects 12 Step Meeting List: from n/a through 3.14.28.	4.3	More Details
CVE-2024-32081	Missing Authorization vulnerability in Websupporter Filter Custom Fields & Taxonomies Light.This issue affects Filter Custom Fields & Taxonomies Light: from n/a through 1.05.	4.3	More Details
CVE-2024-5256	Sonos Era 100 SMB2 Message Handling Integer Underflow Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of Sonos Era 100 smart speakers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of SMB2 messages. The issue results from the lack of proper validation of user-supplied data, which can result in an integer underflow before reading from memory. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-22336.	4.3	More Details
CVE-2024-32701	Missing Authorization vulnerability in InstaWP Team InstaWP Connect.This issue affects InstaWP Connect: from n/a through 0.1.0.24.	4.3	More Details
CVE-2024-5489	The Wbcom Designs – Custom Font Uploader plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'cfu_delete_customfont' function in all versions up to, and including, 2.3.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete any custom font.	4.3	More Details
CVE-2024-33850	Pexip Infinity before 34.1 has Improper Access Control for persons in a waiting room. They can see the conference roster list, and perform certain actions that should not be allowed before they are admitted to the meeting.	4.3	More Details
CVE-2024-4788	The Boostify Header Footer Builder for Elementor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the create_bhf_post function in all versions up to, and including, 1.3.3. This makes it possible for authenticated attackers, with subscriber-level access and above, to create pages or posts with arbitrary content.	4.3	More Details
CVE-2023-6748	The Custom Field Template plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.6.1 via the 'cft' shortcode. This makes it possible for authenticated attackers with contributor access and above, to extract sensitive data including arbitrary post metadata.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0912	Under certain circumstances the Microsoft® Internet Information Server (IIS) used to host the C•CURE 9000 Web Server will log Microsoft Windows credential details within logs. There is no impact to non-web service interfaces C•CURE 9000 or prior versions	4.2	More Details
CVE-2024-5770	The WP Force SSL & HTTPS SSL Redirect plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ajax_save_setting' function in versions up to, and including, 1.66. This makes it possible for authenticated attackers, subscriber-level permissions and above, to update the plugin settings.	4.2	More Details
CVE-2024-28024	A vulnerability exists in the FOXMAN-UN/UNEM in which sensitive information is stored in cleartext within a resource that might be accessible to another control sphere.	4.1	More Details
CVE-2024-37162	zsa is a library for building typesafe server actions in Next.js. All users are impacted. The zsa application transfers the parse error stack from the server to the client in production build mode. This can potentially reveal sensitive information about the server environment, such as the machine username and directory paths. An attacker could exploit this vulnerability to gain unauthorized access to sensitive server information. This information could be used to plan further attacks or gain a deeper understanding of the server infrastructure. This has been patched on `0.3.3`.	4.0	More Details
CVE-2024-36795	Insecure permissions in Netgear WNR614 JNR1010V2/N300-V1.1.0.54_1.0.1 allows attackers to access URLs and directories embedded within the firmware via unspecified vectors.	4.0	More Details
CVE-2024-37161	MeterSphere is an open source continuous testing platform. Prior to version 1.10.1-lts, the system's step editor stores cross-site scripting vulnerabilities. Version 1.10.1-lts fixes this issue.	4.0	More Details
CVE-2024-35749	Authentication Bypass by Spoofing vulnerability in Acurax Under Construction / Maintenance Mode from Acurax allows Authentication Bypass.This issue affects Under Construction / Maintenance Mode from Acurax: from n/a through 2.6.	3.7	More Details
CVE-2023-50803	An issue was discovered in Samsung Mobile Processor, and Modem Exynos 9820, Exynos 9825, Exynos 980, Exynos 990, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos Modem 5123, Exynos Modem 5300. The baseband software does not properly check replay protection specified by the NAS (Non-Access-Stratum) module. This can lead to denial of service.	3.7	More Details
CVE-2024-30512	Missing Authorization vulnerability in weForms.This issue affects weForms: from n/a through 1.6.20.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34684	On Unix, SAP BusinessObjects Business Intelligence Platform (Scheduling) allows an authenticated attacker with administrator access on the local server to access the password of a local account. As a result, an attacker can obtain non-administrative user credentials, which will allow them to read or modify the remote server files.	3.7	More Details
CVE-2023-50804	An issue was discovered in Samsung Mobile Processor, and Modem Exynos 9820, Exynos 9825, Exynos 980, Exynos 990, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos Modem 5123, Exynos Modem 5300. The baseband software does not properly check format types specified by the NAS (Non-Access-Stratum) module. This can lead to bypass of authentication.	3.7	More Details
CVE-2024-5657	The CraftCMS plugin Two-Factor Authentication in versions 3.3.1, 3.3.2 and 3.3.3 discloses the password hash of the currently authenticated user after submitting a valid TOTP.	3.7	More Details
CVE-2024-36407	SuiteCRM is an open-source Customer Relationship Management (CRM) software application. In versions prior to 7.14.4 and 8.6.1, a user password can be reset from an unauthenticated attacker. The attacker does not get access to the new password. But this can be annoying for the user. This attack is also dependent on some password reset functionalities being enabled. It also requires the system using php 7, which is not an officially supported version. Versions 7.14.4 and 8.6.1 contain a fix for this issue.	3.7	More Details
CVE-2024-32873	Evmos is the Ethereum Virtual Machine (EVM) Hub on the Cosmos Network. The spendable balance is not updated properly when delegating vested tokens. The issue allows a clawback vesting account to anticipate the release of unvested tokens. This vulnerability is fixed in 18.0.0.	3.5	More Details
CVE-2024-5829	A vulnerability classified as problematic was found in smallweigit Avue up to 3.4.4. Affected by this vulnerability is an unknown functionality of the component avueUeditor. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-267895. NOTE: The code maintainer explains, that "rich text is no longer maintained".	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5851	A vulnerability classified as problematic has been found in playSMS up to 1.4.7. Affected is an unknown function of the file /index.php?app=main&inc=feature_schedule&op=list of the component SMS Schedule Handler. The manipulation of the argument name/message leads to basic cross site scripting. It is possible to launch the attack remotely. Upgrading to version 1.4.8 is able to address this issue. The name of the patch is 7a88920f6b536c6a91512e739bcb4e8adefeed2b. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-267912. NOTE: The code maintainer was contacted early about this disclosure and was eager to prepare a fix as quickly as possible.	3.5	More Details
CVE-2024-5812	A low severity vulnerability in BIPS has been identified where an attacker with high privileges or a compromised high privilege account can overwrite Read-Only smart rules via a specially crafted API request.	3.3	More Details
CVE-2024-5307	Kofax Power PDF AcroForm Annotation Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Kofax Power PDF. 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 Annotation objects in AcroForms. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-22933.	3.3	More Details
CVE-2024-2213	An issue was discovered in zenml-io/zenml versions up to and including 0.55.4. Due to improper authentication mechanisms, an attacker with access to an active user session can change the account password without needing to know the current password. This vulnerability allows for unauthorized account takeover by bypassing the standard password change verification process. The issue was fixed in version 0.56.3.	3.3	More Details
CVE-2023-38533	A vulnerability has been identified in TIA Administrator (All versions < V3 SP2). The affected component creates temporary download files in a directory with insecure permissions. This could allow any authenticated attacker on Windows to disrupt the update process.	3.3	More Details
CVE-2024-27799	This issue was addressed with additional entitlement checks. This issue is fixed in macOS Sonoma 14.5, macOS Ventura 13.6.7, macOS Monterey 12.7.5, iOS 16.7.8 and iPadOS 16.7.8. An unprivileged app may be able to log keystrokes in other apps including those using secure input mode.	3.3	More Details
CVE-2024-27845	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in iOS 17.5 and iPadOS 17.5. An app may be able to access Notes attachments.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2032	A race condition vulnerability exists in zenml-io/zenml versions up to and including 0.55.3, which allows for the creation of multiple users with the same username when requests are sent in parallel. This issue was fixed in version 0.55.5. The vulnerability arises due to insufficient handling of concurrent user creation requests, leading to data inconsistencies and potential authentication problems. Specifically, concurrent processes may overwrite or corrupt user data, complicating user identification and posing security risks. This issue is particularly concerning for APIs that rely on usernames as input parameters, such as PUT /api/v1/users/test_race, where it could lead to further complications.	3.1	More Details
CVE-2024-22261	SQL-Injection in Harbor allows priviledge users to leak the task IDs	2.7	More Details
CVE-2024-27819	The issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 17.5 and iPadOS 17.5. An attacker with physical access may be able to access contacts from the lock screen.	2.4	More Details
CVE-2024-27814	This issue was addressed through improved state management. This issue is fixed in watchOS 10.5. A person with physical access to a device may be able to view contact information from the lock screen.	2.4	More Details
CVE-2024-5766	A vulnerability was found in Likeshop up to 2.5.7 and classified as problematic. This issue affects some unknown processing of the file /admin of the component Merchandise Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-267449 was assigned to this vulnerability.	2.4	More Details
CVE-2024-21754	A use of password hash with insufficient computational effort vulnerability [CWE-916] affecting FortiOS version 7.4.3 and below, 7.2 all versions, 7.0 all versions, 6.4 all versions and FortiProxy version 7.4.2 and below, 7.2 all versions, 7.0 all versions, 2.0 all versions may allow a privileged attacker with super-admin profile and CLI access to decrypting the backup file.	1.8	More Details
CVE-2024-5609	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-6966. Reason: This candidate is a reservation duplicate of CVE-2023-6966. Notes: All CVE users should reference CVE-2023-6966 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4403	A Cross-Site Request Forgery (CSRF) vulnerability exists in the restart_program function of the parisneo/lollms-webui v9.6. This vulnerability allows attackers to trick users into performing unintended actions, such as resetting the program without their knowledge, by sending specially crafted CSRF forms. This issue affects the installation process, including the installation of Binding zoo and Models zoo, by unexpectedly resetting programs. The vulnerability is due to the lack of CSRF protection in the affected function.	N/A	More Details
CVE-2024-5480	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-35307	Argument Injection Leading to Remote Code Execution in Realtime Graph Extension, allowing unauthenticated attackers to execute arbitrary code on the server. This issue affects Pandora FMS: from 700 through <777.	N/A	More Details
CVE-2024-35306	OS Command injection in Ajax PHP files via HTTP Request, allows to execute system commands by exploiting variables. This issue affects Pandora FMS: from 700 through <777.	N/A	More Details
CVE-2024-35305	Unauth Time-Based SQL Injection in API allows to exploit HTTP request Authorization header. This issue affects Pandora FMS: from 700 through <777.	N/A	More Details
CVE-2020-35154	Rejected reason: CVE ID was once reserved, but never used.	N/A	More Details
CVE-2020-35153	Rejected reason: CVE ID was once reserved, but never used.	N/A	More Details
CVE-2024-35304	System command injection through Netflow function due to improper input validation, allowing attackers to execute arbitrary system commands. This issue affects Pandora FMS: from 700 through <777.	N/A	More Details
CVE-2024-5089	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-5656	Rejected reason: ** REJECT ** Accidental duplicate assignment of CVE-2024-4755. Please use CVE-2024-4755.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6734	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-33679. Reason: This candidate is a reservation duplicate of CVE-2024-33679. Notes: All CVE users should reference CVE-2024-33679 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-5132	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-3380	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-2462	Allow attackers to intercept or falsify data exchanges between the client and the server	N/A	More Details
CVE-2024-2461	If exploited an attacker could traverse the file system to access files or directories that would otherwise be inaccessible	N/A	More Details
CVE-2020-27355	Rejected reason: CVE ID was once reserved, but never used.	N/A	More Details
CVE-2024-5825	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-5398	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-4387	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-4206	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-4155	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-2024-31631	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2024-35329	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-2024-31630	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2024-29855	Hard-coded JWT secret allows authentication bypass in Veeam Recovery Orchestrator	N/A	More Details
CVE-2024-31629	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2024-31628	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2024-31627	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2024-31626	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2024-31625	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2024-31624	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36970	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: Use request_module_nowait This appears to work around a deadlock regression that came in with the LED merge in 6.9. The deadlock happens on my system with 24 iwlwifi radios, so maybe it something like all worker threads are busy and some work that needs to complete cannot complete. [also remove unnecessary "load_module" var and now-wrong comment]	N/A	More Details
CVE-2024-31623	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2024-31622	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2024-36966	In the Linux kernel, the following vulnerability has been resolved: erofs: reliably distinguish block based and fscache mode When erofs_kill_sb() is called in block dev based mode, s_bdev may not have been initialised yet, and if CONFIG_EROFS_FS_ONDEMAND is enabled, it will be mistaken for fscache mode, and then attempt to free an anon_dev that has never been allocated, triggering the following warning: ========== ida_free called for id=0 which is not allocated. WARNING: CPU: 14 PID: 926 at lib/idr.c:525 ida_free+0x134/0x140 Modules linked in: CPU: 14 PID: 926 Comm: mount Not tainted 6.9.0-rc3-dirty #630 RIP: 0010:ida_free+0x134/0x140 Call Trace: <TASK> erofs_kill_sb+0x81/0x90 deactivate_locked_super+0x35/0x80 get_tree_bdev+0x136/0x1e0 vfs_get_tree+0x2c/0xf0 do_new_mount+0x190/0x2f0 [...] ========== Now when erofs_kill_sb() is called, erofs_sb_info must have been initialised, so use sbi->fsid to distinguish between the two modes.	N/A	More Details
CVE-2024-5758	Rejected reason: ** REJECT ** Duplicate of CVE-2024-4305. Please use CVE-2024-4305 instead.	N/A	More Details
CVE-2024-5761	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: [CVE-2024-5260]. Reason: This candidate is a reservation duplicate of [CVE-2024-5260]. Notes: All CVE users should reference [CVE-ID] instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-3133	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-2024-36811	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-37295. Reason: This candidate is a reservation duplicate of CVE-2024-37295. Notes: All CVE users should reference CVE-2024-37295 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-23595	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-6997	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-4152	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2020-27354	Rejected reason: CVE ID was once reserved, but never used.	N/A	More Details