SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 03 July 2024

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-39251	An issue in the component ControlCenter.sys/ControlCenter64.sys of ThundeRobot Control Center v2.0.0.10 allows attackers to access sensitive information, execute arbitrary code, or escalate privileges via sending crafted IOCTL requests.	10.0	More Details
CVE-2023-41918	A vulnerability allows unauthorized access to functionality inadequately constrained by ACLs. Attackers may exploit this to unauthenticated execute commands potentially leading to unauthorized data manipulation, access to privileged functions, or even the execution of arbitrary code.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2973	An Authentication Bypass Using an Alternate Path or Channel vulnerability in Juniper Networks Session Smart Router or conductor running with a redundant peer allows a network based attacker to bypass authentication and take full control of the device. Only routers or conductors that are running in high-availability redundant configurations are affected by this vulnerability. No other Juniper Networks products or platforms are affected by this issue. This issue affects: Session Smart Router: * All versions before 5.6.15, * from 6.0 before 6.1.9-lts, * from 6.2 before 6.2.5-sts. Session Smart Conductor: * All versions before 5.6.15, * from 6.0 before 6.1.9-lts, * from 6.2 before 6.2.5-sts. WAN Assurance Router: * 6.0 versions before 6.1.9-lts, * 6.2 versions before 6.2.5-sts.	10.0	More Details
CVE-2024-6071	PTC Creo Elements/Direct License Server exposes a web interface which can be used by unauthenticated remote attackers to execute arbitrary OS commands on the server.	10.0	More Details
CVE-2024-38366	trunk.cocoapods.org is the authentication server for the CoacoaPods dependency manager. The part of trunk which verifies whether a user has a real email address on signup used a rfc-822 library which executes a shell command to validate the email domain MX records validity. It works via an DNS MX. This lookup could be manipulated to also execute a command on the trunk server, effectively giving root access to the server and the infrastructure. This issue was patched server-side with commit 001cc3a430e75a16307f5fd6cdff1363ad2f40f3 in September 2023. This RCE triggered a full user-session reset, as an attacker could have used this method to write to any Podspec in trunk.	10.0	More Details
CVE-2023-41917	Inadequate input validation exposes the system to potential remote code execution (RCE) risks. Attackers can exploit this vulnerability by appending shell commands to the Speed-Measurement feature, enabling unauthorized code execution.	10.0	More Details
CVE-2024-39008	robinweser fast-loops v1.1.3 was discovered to contain a prototype pollution via the function objectMergeDeep. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	10.0	More Details
CVE-2024-38999	jrburke requirejs v2.3.6 was discovered to contain a prototype pollution via the function s.contexts._.configure. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1839	Intrado 911 Emergency Gateway login form is vulnerable to an unauthenticated blind time-based SQL injection, which may allow an unauthenticated remote attacker to execute malicious code, exfiltrate data, or manipulate the database.	10.0	More Details
CVE-2024-38513	Fiber is an Express-inspired web framework written in Go A vulnerability present in versions prior to 2.52.5 is a session middleware issue in GoFiber versions 2 and above. This vulnerability allows users to supply their own session_id value, resulting in the creation of a session with that key. If a website relies on the mere presence of a session for security purposes, this can lead to significant security risks, including unauthorized access and session fixation attacks. All users utilizing GoFiber's session middleware in the affected versions are impacted. The issue has been addressed in version 2.52.5. Users are strongly encouraged to upgrade to version 2.52.5 or higher to mitigate this vulnerability. Users who are unable to upgrade immediately can apply the following workarounds to reduce the risk: Either implement additional validation to ensure session IDs are not supplied by the user and are securely generated by the server, or regularly rotate session IDs and enforce strict session expiration policies.	10.0	More Details
CVE-2024-37762	MachForm up to version 21 is affected by an authenticated unrestricted file upload which leads to a remote code execution.	9.9	More Details
CVE-2024-3330	Vulnerability in Spotfire Spotfire Analyst, Spotfire Spotfire Server, Spotfire Spotfire for AWS Marketplace allows In the case of the installed Windows client: Successful execution of this vulnerability will result in an attacker being able to run arbitrary code.This requires human interaction from a person other than the attacker., In the case of the Web player (Business Author): Successful execution of this vulnerability via the Web Player, will result in the attacker being able to run arbitrary code as the account running the Web player process, In the case of Automation Services: Successful execution of this vulnerability will result in an attacker being able to run arbitrary code via Automation Services..This issue affects Spotfire Analyst: from 12.0.9 through 12.5.0, from 14.0 through 14.0.2; Spotfire Server: from 12.0.10 through 12.5.0, from 14.0 through 14.0.3, from 14.2.0 through 14.3.0; Spotfire for AWS Marketplace: from 14.0 before 14.3.0.	9.9	More Details
CVE-2024-39013	2o3t-utility v0.1.2 was discovered to contain a prototype pollution via the function extend. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39014	ahilfoley cahil/utils v2.3.2 was discovered to contain a prototype pollution via the function set. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	9.8	More Details
CVE-2024-38474	Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.	9.8	More Details
CVE-2024-39015	cafebazaar hod v0.4.14 was discovered to contain a prototype pollution via the function request. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	9.8	More Details
CVE-2024-39017	agreejs shared v0.0.1 was discovered to contain a prototype pollution via the function mergeInternalComponents. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	9.8	More Details
CVE-2024-36401	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.23.6, 2.24.4, and 2.25.2, multiple OGC request parameters allow Remote Code Execution (RCE) by unauthenticated users through specially crafted input against a default GeoServer installation due to unsafely evaluating property names as XPath expressions. The GeoTools library API that GeoServer calls evaluates property/attribute names for feature types in a way that unsafely passes them to the commons-jxpath library which can execute arbitrary code when evaluating XPath expressions. This XPath evaluation is intended to be used only by complex feature types (i.e., Application Schema data stores) but is incorrectly being applied to simple feature types as well which makes this vulnerability apply to **ALL** GeoServer instances. No public PoC is provided but this vulnerability has been confirmed to be exploitable through WFS GetFeature, WFS GetPropertyValue, WMS GetMap, WMS GetFeatureInfo, WMS GetLegendGraphic and WPS Execute requests. This vulnerability can lead to executing arbitrary code. Versions 2.23.6, 2.24.4, and 2.25.2 contain a patch for the issue. A workaround exists by removing the `gt-complex-x.y.jar` file from the GeoServer where `x.y` is the GeoTools version (e.g., `gt-complex-31.1.jar` if running GeoServer 2.25.1). This will remove the vulnerable code from GeoServer but may break some GeoServer functionality or prevent GeoServer from deploying if the gt-complex module is needed.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38998	jrburke requirejs v2.3.6 was discovered to contain a prototype pollution via the function config. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	9.8	More Details
CVE-2024-38996	ag-grid-community v31.3.2 and ag-grid-enterprise v31.3.2 were discovered to contain a prototype pollution via the _.mergeDeep function. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	9.8	More Details
CVE-2024-38476	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue.	9.8	More Details
CVE-2024-39236	Gradio v4.36.1 was discovered to contain a code injection vulnerability via the component /gradio/component_meta.py. This vulnerability is triggered via a crafted input. NOTE: the supplier disputes this because the report is about a user attacking himself.	9.8	More Details
CVE-2024-38993	rjrodger jsonic-next v2.12.1 was discovered to contain a prototype pollution via the function empty. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	9.8	More Details
CVE-2024-39309	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. A vulnerability in versions prior to 6.5.7 and 7.1.0 allows SQL injection when Parse Server is configured to use the PostgreSQL database. The algorithm to detect SQL injection has been improved in versions 6.5.7 and 7.1.0. No known workarounds are available.	9.8	More Details
CVE-2024-6172	The Email Subscribers by Icegram Express – Email Marketing, Newsletters, Automation for WordPress & WooCommerce plugin for WordPress is vulnerable to time-based SQL Injection via the db parameter in all versions up to, and including, 5.7.25 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-2023-41919	Hardcoded credentials are discovered within the application's source code, creating a potential security risk for unauthorized access.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41920	The vulnerability allows attackers access to the root account without having to authenticate. Specifically, if the device is configured with the IP address of 10.10.10.10, the root user is automatically logged in.	9.8	More Details
CVE-2023-41921	A vulnerability allows attackers to download source code or an executable from a remote location and execute the code without sufficiently verifying the origin and integrity of the code. This vulnerability can allow attackers to modify the firmware before uploading it to the system, thus achieving the modification of the target's integrity to achieve an insecure state.	9.8	More Details
CVE-2024-36404	GeoTools is an open source Java library that provides tools for geospatial data. Prior to versions 31.2, 30.4, and 29.6, Remote Code Execution (RCE) is possible if an application uses certain GeoTools functionality to evaluate XPath expressions supplied by user input. Versions 31.2, 30.4, and 29.6 contain a fix for this issue. As a workaround, GeoTools can operate with reduced functionality by removing the `gt-complex` jar from one's application. As an example of the impact, application schema `datastore` would not function without the ability to use XPath expressions to query complex content. Alternatively, one may utilize a drop-in replacement GeoTools jar from SourceForge for versions 31.1, 30.3, 30.2, 29.2, 28.2, 27.5, 27.4, 26.7, 26.4, 25.2, and 24.0. These jars are for download only and are not available from maven central, intended to quickly provide a fix to affected applications.	9.8	More Details
CVE-2023-24531	Command go env is documented as outputting a shell script containing the Go environment. However, go env doesn't sanitize values, so executing its output as a shell script can cause various bad bahaviors, including executing arbitrary commands or inserting new environment variables. This issue is relatively minor because, in general, if an attacker can set arbitrary environment variables on a system, they have better attack vectors than making "go env" print them out.	9.8	More Details
CVE-2024-4228	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), CWE - 200 - Exposure of Sensitive Information to an Unauthorized Actor, CWE - 522 - Insufficiently Protected Credentials vulnerability in Magarsus Consultancy SSO (Single Sign On) allows SQL Injection.This issue affects SSO (Single Sign On): from 1.0 before 1.1.	9.8	More Details
CVE-2024-4708	mySCADA myPRO uses a hard-coded password which could allow an attacker to remotely execute code on the affected device.	9.8	More Details
CVE-2024-20080	In gnss service, there is a possible escalation of privilege due to improper certificate validation. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08720039; Issue ID: MSV-1424.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36072	Netwrix CoSoSys Endpoint Protector through 5.9.3 and CoSoSys Unify through 7.0.6 contain a remote code execution vulnerability in the logging component of the Endpoint Protector and Unify server application which allows an unauthenticated remote attacker to send a malicious request, resulting in the ability to execute system commands with root privileges.	9.8	More Details
CVE-2024-39243	An issue discovered in skycaiji 2.8 allows attackers to run arbitrary code via crafted POST request to /index.php?s=/admin/develop/editor_save.	9.8	More Details
CVE-2024-37734	An issue in OpenEMR 7.0.2 allows a remote attacker to escalate privileges viaa crafted POST request using the noteid parameter.	9.8	More Details
CVE-2024-0947	Reliance on Cookies without Validation and Integrity Checking vulnerability in Talya Informatics Elektraweb allows Session Credential Falsification through Manipulation, Accessing/Intercepting/Modifying HTTP Cookies, Manipulating Opaque Client-based Data Tokens.This issue affects Elektraweb: before v17.0.68.	9.8	More Details
CVE-2024-0949	Improper Access Control, Missing Authorization, Incorrect Authorization, Incorrect Permission Assignment for Critical Resource, Missing Authentication, Weak Authentication, Improper Restriction of Communication Channel to Intended Endpoints vulnerability in Talya Informatics Elektraweb allows Exploiting Incorrectly Configured Access Control Security Levels, Manipulating Web Input to File System Calls, Embedding Scripts within Scripts, Malicious Logic Insertion, Modification of Windows Service Configuration, Malicious Root Certificate, Intent Spoof, WebView Exposure, Data Injected During Configuration, Incomplete Data Deletion in a Multi-Tenant Environment, Install New Service, Modify Existing Service, Install Rootkit, Replace File Extension Handlers, Replace Trusted Executable, Modify Shared File, Add Malicious File to Shared Webroot, Run Software at Logon, Disable Security Software.This issue affects Elektraweb: before v17.0.68.	9.8	More Details
CVE-2024-39374	TELSAT marKoni FM Transmitters are vulnerable to an attacker exploiting a hidden admin account that can be accessed through the use of hard-coded credentials.	9.8	More Details
CVE-2024-39375	TELSAT marKoni FM Transmitters are vulnerable to an attacker bypassing authentication and gaining administrator privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39376	TELSAT marKoni FM Transmitters are vulnerable to users gaining unauthorized access to sensitive information or performing actions beyond their designated permissions.	9.8	More Details
CVE-2024-39669	In the Console in Soffid IAM before 3.5.39, necessary checks were not applied to some Java objects. A malicious agent could possibly execute arbitrary code in the Sync Server and compromise security.	9.8	More Details
CVE-2024-5751	BerriAI/litellm version v1.35.8 contains a vulnerability where an attacker can achieve remote code execution. The vulnerability exists in the `add_deployment` function, which decodes and decrypts environment variables from base64 and assigns them to `os.environ`. An attacker can exploit this by sending a malicious payload to the `/config/update` endpoint, which is then processed and executed by the server when the `get_secret` function is triggered. This requires the server to use Google KMS and a database to store a model.	9.8	More Details
CVE-2024-20078	In venc, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08737250; Issue ID: MSV-1452.	9.8	More Details
CVE-2024-6127	BC Security Empire before 5.9.3 is vulnerable to a path traversal issue that can lead to remote code execution. A remote, unauthenticated attacker can exploit this vulnerability over HTTP by acting as a normal agent, completing all cryptographic handshakes, and then triggering an upload of payload data containing a malicious path.	9.8	More Details
CVE-2024-39208	luci-app-lucky v2.8.3 was discovered to contain hardcoded credentials.	9.8	More Details
CVE-2024-3816	Sites managed in S@M CMS (Concept Intermedia) might be vulnerable to a blind SQL Injection executed using the search bar. Only a part of observed services is vulnerable, but since vendor has not investigated the root problem, it is hard to determine when the issue appears.	9.8	More Details
CVE-2024-39704	Soft Circle French-Bread Melty Blood: Actress Again: Current Code through 1.07 Rev. 1.4.0 allows a remote attacker to execute arbitrary code on a client's machine via a crafted packet on TCP port 46318.	9.8	More Details
CVE-2024-39705	NLTK through 3.8.1 allows remote code execution if untrusted packages have pickled Python code, and the integrated data package download functionality is used. This affects, for example, averaged_perceptron_tagger and punkt.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39349	A vulnerability regarding buffer copy without checking size of input ('Classic Buffer Overflow') is found in the libjansson component and it does not affect the upstream library. This allows remote attackers to execute arbitrary code via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	9.8	More Details
CVE-2024-6265	The UsersWP – Front-end login form, User Registration, User Profile & Members Directory plugin for WordPress plugin for WordPress is vulnerable to time-based SQL Injection via the ‘uwp_sort_by’ parameter in all versions up to, and including, 1.2.10 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-2024-5655	An issue was discovered in GitLab CE/EE affecting all versions starting from 15.8 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows an attacker to trigger a pipeline as another user under certain circumstances.	9.6	More Details
CVE-2024-36059	Directory Traversal vulnerability in Kalkitech ASE ASE61850 IEDSmart upto and including version 2.3.5 allows attackers to read/write arbitrary files via the IEC61850 File Transfer protocol.	9.4	More Details
CVE-2024-6424	External server-side request vulnerability in MESbook 20221021.03 version, which could allow a remote, unauthenticated attacker to exploit the endpoint "/api/Proxy/Post?userName=&password=&uri=<FILEIINTERNAL URLIIP/HOST" or "/api/Proxy/Get?userName=&password=&uri=<ARCHIVOIURL INTERNAIIP/HOST" to read the source code of web files, read internal files or access network resources.	9.3	More Details
CVE-2024-38368	trunk.cocoapods.org is the authentication server for the CoacoaPods dependency manager. A vulnerability affected older pods which migrated from the pre-2014 pull request workflow to trunk. If the pods had never been claimed then it was still possible to do so. It was also possible to have all owners removed from a pod, and that made the pod available for the same claiming system. This was patched server-side in commit 71be5440906b6bdfbc0bcc7f8a9fec33367ea0f4 in September 2023.	9.3	More Details
CVE-2024-37252	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Icegram Email Subscribers & Newsletters allows SQL Injection.This issue affects Email Subscribers & Newsletters: from n/a through 5.7.25.	9.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5322	The N-central server is vulnerable to session rebinding of already authenticated users when using Entra SSO, which can lead to authentication bypass. This vulnerability is present in all Entra-supported deployments of N-central prior to 2024.3.	9.1	More Details
CVE-2024-38475	Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure. Substitutions in server context that use a backreferences or variables as the first segment of the substitution are affected. Some unsafe RewiteRules will be broken by this change and the rewrite flag "UnsafePrefixStat" can be used to opt back in once ensuring the substitution is appropriately constrained.	9.1	More Details
CVE-2024-5535	Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash. In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the	9.1	More Details

CVE Number	Description	Base Score	Reference
	SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a "no overlap" response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available.		
CVE-2024-37371	In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can cause invalid memory reads during GSS message token handling by sending message tokens with invalid length fields.	9.1	More Details
CVE-2019-25211	parseWildcardRules in Gin-Gonic CORS middleware before 1.6.0 mishandles a wildcard at the end of an origin string, e.g., https://example.community/* is allowed when the intention is that only https://example.com/* should be allowed, and http://localhost.example.com/* is allowed when the intention is that only http://localhost/* should be allowed.	9.1	More Details
CVE-2024-6425	Incorrect Provision of Specified Functionality vulnerability in MESbook 20221021.03 version. An unauthenticated remote attacker can register user accounts without being authenticated from the route "/account/Register/" and in the parameters "UserName= <RANDOMUSER>&Password=<PASSWORD>&ConfirmPassword= <PASSWORD-REPEAT>".	9.1	More Details
CVE-2024-32755	Under certain circumstances the web interface will accept characters unrelated to the expected input.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28200	The N-central server is vulnerable to an authentication bypass of the user interface. This vulnerability is present in all deployments of N-central prior to 2024.2. This vulnerability was discovered through internal N-central source code review and N-able has not observed any exploitation in the wild.	9.1	More Details
CVE-2024-39848	Internet2 Grouper before 5.6 allows authentication bypass when LDAP authentication is used in certain ways. This is related to internet2.middleware.grouper.ws.security.WsGrouperLdapAuthentication and the use of the UyY29r password for the M3vwHr account. This also affects "Grouper for Web Services" before 4.13.1.	9.1	More Details
CVE-2024-29039	tpm2 is the source repository for the Trusted Platform Module (TPM2.0) tools. This vulnerability allows attackers to manipulate tpm2_checkquote outputs by altering the TPML_PCR_SELECTION in the PCR input file. As a result, digest values are incorrectly mapped to PCR slots and banks, providing a misleading picture of the TPM state. This issue has been patched in version 5.7.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-36984	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 on Windows, an authenticated user could execute a specially crafted query that they could then use to serialize untrusted data. The attacker could use the query to execute arbitrary code.	8.8	More Details
CVE-2024-37905	authentik is an open-source Identity Provider that emphasizes flexibility and versatility. Authentik API-Access-Token mechanism can be exploited to gain admin user privileges. A successful exploit of the issue will result in a user gaining full admin access to the Authentik application, including resetting user passwords and more. This issue has been patched in version(s) 2024.2.4, 2024.4.2 and 2024.6.0.	8.8	More Details
CVE-2024-28984	Hitachi Vantara Pentaho Business Analytics Server prior to versions 10.1.0.0 and 9.3.0.7, including 8.3.x allow a malicious URL to inject content into the Analyzer plugin interface.	8.8	More Details
CVE-2024-28983	Hitachi Vantara Pentaho Business Analytics Server prior to versions 10.1.0.0 and 9.3.0.7, including 8.3.x allow a malicious URL to inject content into the Analyzer plugin interface.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6054	The Auto Featured Image plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'create_post_attachment_from_url' function in all versions up to, and including, 1.2. This makes it possible for authenticated attackers, with contributor-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2024-36985	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10, a low-privileged user that does not hold the admin or power Splunk roles could cause a Remote Code Execution through an external lookup that references the “splunk_archiver“ application.	8.8	More Details
CVE-2024-38991	akbr patch-into v1.0.1 was discovered to contain a prototype pollution via the function patchInto. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	8.8	More Details
CVE-2024-38992	airvertco frappejs v0.0.11 was discovered to contain a prototype pollution via the function registerView. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	8.8	More Details
CVE-2024-4007	Default credential in install package in ABB ASPECT; NEXUS Series; MATRIX Series version 3.07 allows attacker to login to product instances wrongly configured.	8.8	More Details
CVE-2024-5767	The sitetweet WordPress plugin through 0.2 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	8.8	More Details
CVE-2024-38521	Hush Line is a free and open-source, anonymous-tip-line-as-a-service for organizations or individuals. There is a stored XSS in the Inbox. The input is displayed using the `safe` Jinja2 attribute, and thus not sanitized upon display. This issue has been patched in version 0.1.0.	8.8	More Details
CVE-2024-5606	The Quiz and Survey Master (QSM) WordPress plugin before 9.0.2 is vulnerable does not validate and escape the question_id parameter in the qsm_bulk_delete_question_from_database AJAX action, leading to a SQL injection exploitable by Contributors and above role	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5349	The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.3.8.1 via the 'map_style' parameter. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	8.8	More Details
CVE-2024-37140	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain an OS command injection vulnerability in an admin operation. A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the system application's underlying OS with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker.	8.8	More Details
CVE-2023-41926	The webserver utilizes basic authentication for its user login to the configuration interface. As encryption is disabled on port 80, it enables potential eavesdropping on user traffic, making it possible to intercept their credentials.	8.8	More Details
CVE-2024-23736	Cross Site Request Forgery (CSRF) vulnerability in savignano S/Notify before 4.0.2 for Confluence allows attackers to manipulate a user's S/MIME certificate of PGP key via malicious link or email.	8.8	More Details
CVE-2024-39154	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/keyWord_deal.php?mudi=del&dataType=word&dataTypeCN.	8.8	More Details
CVE-2024-39158	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/userSys_deal.php?mudi=infoSet.	8.8	More Details
CVE-2024-23767	An issue was discovered on HMS Anybus X-Gateway AB7832-F firmware version 3. The HICP protocol allows unauthenticated changes to a device's network configurations.	8.8	More Details
CVE-2024-29176	Dell PowerProtect DD, version(s) 8.0, 7.13.1.0, 7.10.1.30, 7.7.5.40, contain(s) an Out-of-bounds Write vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Code execution.	8.8	More Details
CVE-2024-1107	Authorization Bypass Through User-Controlled Key vulnerability in Talya Informatics Travel APPS allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Travel APPS: before v17.0.68.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37765	Machform up to version 19 is affected by an authenticated Blind SQL injection in the user account settings page.	8.8	More Details
CVE-2024-39840	Factorio before 1.1.101 allows a crafted server to execute arbitrary code on clients via a custom map that leverages the ability of certain Lua base module functions to execute bytecode and generate fake objects.	8.8	More Details
CVE-2024-2386	The WordPress Plugin for Google Maps – WP MAPS plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter of the 'put_wpgm' shortcode in all versions up to, and including, 4.6.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2024-4901	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.9 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, where a stored XSS vulnerability could be imported from a project with malicious commit notes.	8.7	More Details
CVE-2024-38371	authentik is an open-source Identity Provider. Access restrictions assigned to an application were not checked when using the OAuth2 Device code flow. This could potentially allow users without the correct authorization to get OAuth tokens for an application and access it. This issue has been patched in version(s) 2024.6.0, 2024.2.4 and 2024.4.3.	8.6	More Details
CVE-2024-5885	stangirard/quivr version 0.0.236 contains a Server-Side Request Forgery (SSRF) vulnerability. The application does not provide sufficient controls when crawling a website, allowing an attacker to access applications on the local network. This vulnerability could allow a malicious user to gain access to internal servers, the AWS metadata endpoint, and capture Supabase data.	8.6	More Details
CVE-2024-37479	Local File Inclusion vulnerability in LA-Studio LA-Studio Element Kit for Elementor via "LaStudioKit Progress Bar" widget in New Post, specifically in the "progress_type" attribute.This issue affects LA-Studio Element Kit for Elementor: from n/a through 1.3.8.1.	8.5	More Details
CVE-2023-43554	Memory corruption while processing IOCTL handler in FastRPC.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23380	Memory corruption while handling user packets during VBO bind operation.	8.4	More Details
CVE-2024-21461	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	8.4	More Details
CVE-2024-23372	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size.	8.4	More Details
CVE-2024-23373	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released.	8.4	More Details
CVE-2024-32229	FFmpeg 7.0 contains a heap-buffer-overflow at libavfilter/vf_tiltandshift.c:189:5 in copy_column.	8.4	More Details
CVE-2024-4578	This Advisory describes an issue that impacts Arista Wireless Access Points. Any entity with the ability to authenticate via SSH to an affected AP as the “config” user is able to cause a privilege escalation via spawning a bash shell. The SSH CLI session does not require high permissions to exploit this vulnerability, but the config password is required to establish the session. The spawned shell is able to obtain root privileges.	8.4	More Details
CVE-2024-36260	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through out-of-bounds write.	8.2	More Details
CVE-2024-36243	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through out-of-bounds read and write.	8.2	More Details
CVE-2024-37030	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through use after free.	8.2	More Details
CVE-2024-37077	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through out-of-bounds write.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37185	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through out-of-bounds write.	8.2	More Details
CVE-2024-38367	trunk.cocoapods.org is the authentication server for the CoacoaPods dependency manager. Prior to commit d4fa66f49cedab449af9a56a21ab40697b9f7b97, the trunk sessions verification step could be manipulated for owner session hijacking Compromising a victim's session will result in a full takeover of the CocoaPods trunk account. The threat actor could manipulate their pod specifications, disrupt the distribution of legitimate libraries, or cause widespread disruption within the CocoaPods ecosystem. This was patched server-side with commit d4fa66f49cedab449af9a56a21ab40697b9f7b97 in October 2023.	8.2	More Details
CVE-2024-39207	lua-shmem v1.0-1 was discovered to contain a buffer overflow via the shmem_write function.	8.2	More Details
CVE-2024-5460	A vulnerability in the default configuration of the Simple Network Management Protocol (SNMP) feature of Brocade Fabric OS versions before v9.0.0 could allow an authenticated, remote attacker to read data from an affected device via SNMP. The vulnerability is due to hard-coded, default community string in the configuration file for the SNMP daemon. An attacker could exploit this vulnerability by using the static community string in SNMP version 1 queries to an affected device.	8.1	More Details
CVE-2024-5935	A Cross-Site Request Forgery (CSRF) vulnerability in version 0.5.0 of imartinez/privategpt allows an attacker to delete all uploaded files on the server. This can lead to data loss and service disruption for the application's users.	8.1	More Details
CVE-2024-39016	che3vinci c3/utils-1 1.0.131 was discovered to contain a prototype pollution via the function assign. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	8.1	More Details
CVE-2024-37282	It was identified that under certain specific preconditions, an API key that was originally created with a specific privileges could be subsequently used to create new API keys that have elevated privileges.	8.1	More Details
CVE-2024-36997	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312, an admin user could store and execute arbitrary JavaScript code in the browser context of another Splunk user through the conf-web/settings REST endpoint. This could potentially cause a persistent cross-site scripting (XSS) exploit.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6387	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.	8.1	More Details
CVE-2024-38473	Encoding problem in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests. Users are recommended to upgrade to version 2.4.60, which fixes this issue.	8.1	More Details
CVE-2024-27628	Buffer Overflow vulnerability in DCMTK v.3.6.8 allows an attacker to execute arbitrary code via the EctEnhancedCT method component.	8.1	More Details
CVE-2024-36983	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.109 and 9.1.2308.207, an authenticated user could create an external lookup that calls a legacy internal function. The authenticated user could use this internal function to insert code into the Splunk platform installation directory. From there, the user could execute arbitrary code on the Splunk platform Instance.	8.0	More Details
CVE-2024-35260	An authenticated attacker can exploit an untrusted search path vulnerability in Microsoft Dataverse to execute code over a network.	8.0	More Details
CVE-2024-21465	Memory corruption while processing key blob passed by the user.	7.8	More Details
CVE-2024-23368	Memory corruption when allocating and accessing an entry in an SMEM partition.	7.8	More Details
CVE-2023-30997	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could allow a local user to obtain root access due to improper access controls. IBM X-Force ID: 254638.	7.8	More Details
CVE-2023-30998	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could allow a local user to obtain root access due to improper access controls. IBM X-Force ID: 254649.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4679	Incorrect Default Permissions vulnerability in Hitachi JP1/Extensible SNMP Agent for Windows, Hitachi JP1/Extensible SNMP Agent on Windows, Hitachi Job Management Partner1/Extensible SNMP Agent on Windows allows File Manipulation.This issue affects JP1/Extensible SNMP Agent for Windows: from 12-00 before 12-00-01, from 11-00 through 11-00-*; JP1/Extensible SNMP Agent: from 10-10 through 10-10-01, from 10-00 through 10-00-02, from 09-00 through 09-00-04; Job Management Partner1/Extensible SNMP Agent: from 10-10 through 10-10-01, from 10-00 through 10-00-02, from 09-00 through 09-00-04.	7.8	More Details
CVE-2024-32230	FFmpeg 7.0 is vulnerable to Buffer Overflow. There is a negative-size-param bug at libavcodec/mpegvideo_enc.c:1216:21 in load_input_picture in FFmpeg7.0	7.8	More Details
CVE-2022-25478	Vulnerability in Realtek RtsPer driver for PCIe Card Reader (RtsPer.sys) before 10.0.22000.21355 and Realtek RtsUer driver for USB Card Reader (RtsUer.sys) before 10.0.22000.31274 provides read and write access to the PCI configuration space of the device.	7.8	More Details
CVE-2024-34595	Improper access control in clickAdapterItem of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities.	7.8	More Details
CVE-2024-38519	`yt-dlp` and `youtube-dl` are command-line audio/video downloaders. Prior to the fixed versions, `yt-dlp` and `youtube-dl` do not limit the extensions of downloaded files, which could lead to arbitrary filenames being created in the download folder (and path traversal on Windows). Since `yt-dlp` and `youtube-dl` also read config from the working directory (and on Windows executables will be executed from the `yt-dlp` or `youtube-dl` directory), this could lead to arbitrary code being executed. `yt-dlp` version 2024.07.01 fixes this issue by whitelisting the allowed extensions. `youtube-dl` fixes this issue in commit `d42a222` on the `master` branch and in nightly builds tagged 2024-07-03 or later. This might mean some very uncommon extensions might not get downloaded, however it will also limit the possible exploitation surface. In addition to upgrading, have `.%(ext)s` at the end of the output template and make sure the user trusts the websites that they are downloading from. Also, make sure to never download to a directory within PATH or other sensitive locations like one's user directory, `system32`, or other binaries locations. For users who are not able to upgrade, keep the default output template (`-o "%(title)s [%(id)s].%(ext)s`); make sure the extension of the media to download is a common video/audio/sub/... one; try to avoid the generic extractor; and/or use `--ignore-config --config-location ...` to not load config from common locations.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4467	A flaw was found in the QEMU disk image utility (qemu-img) 'info' command. A specially crafted image file containing a `json:{}` value describing block devices in QMP could cause the qemu-img process on the host to consume large amounts of memory or CPU time, leading to denial of service or read/write to an existing external file.	7.8	More Details
CVE-2022-27540	A potential Time-of-Check to Time-of Use (TOCTOU) vulnerability has been identified in the HP BIOS for certain HP PC products, which might allow arbitrary code execution, denial of service, and information disclosure. HP is releasing BIOS updates to mitigate the potential vulnerability.	7.8	More Details
CVE-2024-34122	Acrobat for Edge versions 126.0.2592.68 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-25480	Vulnerability in Realtek RtsPer driver for PCIe Card Reader (RtsPer.sys) before 10.0.22000.21355 and Realtek RtsUer driver for USB Card Reader (RtsUer.sys) before 10.0.22000.31274 allows writing to kernel memory beyond the SystemBuffer of the IRP.	7.8	More Details
CVE-2024-22106	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS).	7.8	More Details
CVE-2024-0153	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in Arm Ltd Valhall GPU Firmware, Arm Ltd Arm 5th Gen GPU Architecture Firmware allows a local non-privileged user to make improper GPU processing operations to access a limited amount outside of buffer bounds. If the operations are carefully prepared, then this in turn could give them access to all system memory. This issue affects Valhall GPU Firmware: from r29p0 through r46p0; Arm 5th Gen GPU Architecture Firmware: from r41p0 through r46p0.	7.8	More Details
CVE-2024-25088	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code.	7.8	More Details
CVE-2024-25086	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4395	The XPC service within the audit functionality of Jamf Compliance Editor before version 1.3.1 on macOS can lead to local privilege escalation.	7.8	More Details
CVE-2024-34585	Improper access control in launchApp of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities.	7.8	More Details
CVE-2024-27629	An issue in dc2niix before v.1.0.20240202 allows a local attacker to execute arbitrary code via the generated file name is not properly escaped and injected into a system call when certain types of compression are used.	7.8	More Details
CVE-2024-20891	Improper access control in launchFullscreenIntent of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities.	7.8	More Details
CVE-2024-20888	Improper access control in OneUIHome prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities. User interaction is required for triggering this vulnerability.	7.8	More Details
CVE-2024-26314	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code.	7.8	More Details
CVE-2023-51776	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code.	7.8	More Details
CVE-2024-5865	Vulnerability in Delinea Centrify PAS v. 21.3 and possibly others. The application is prone to the path traversal vulnerability allowing arbitrary files reading outside the web publish directory. Versions 23.1-HF7 and on have the patch.	7.7	More Details
CVE-2024-20895	Improper access control in Dar service prior to SMR Jul-2024 Release 1 allows local attackers to bypass restriction for calling SDP features.	7.7	More Details
CVE-2024-22232	A specially crafted url can be created which leads to a directory traversal in the salt file server. A malicious user can read an arbitrary file from a Salt master's filesystem.	7.7	More Details
CVE-2024-25943	iDRAC9, versions prior to 7.00.00.172 for 14th Generation and 7.10.50.00 for 15th and 16th Generations, contains a session hijacking vulnerability in IPMI. A remote attacker could potentially exploit this vulnerability, leading to arbitrary code execution on the vulnerable application.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4758	The Muslim Prayer Time BD WordPress plugin through 2.4 does not have CSRF check in place when reseting its settings, which could allow attackers to make a logged in admin reset them via a CSRF attack	7.6	More Details
CVE-2024-37370	In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can modify the plaintext Extra Count field of a confidential GSS krb5 wrap token, causing the unwrapped token to appear truncated to the application.	7.5	More Details
CVE-2024-39134	A Stack Buffer Overflow vulnerability in zziplibv 0.13.77 allows attackers to cause a denial of service via the __zzip_fetch_disk_trailer() function at /zzip/zip.c.	7.5	More Details
CVE-2024-37298	gorilla/schema converts structs to and from form values. Prior to version 1.4.1 Running `schema.Decoder.Decode()` on a struct that has a field of type `[]struct{...}` opens it up to malicious attacks regarding memory allocations, taking advantage of the sparse slice functionality. Any use of `schema.Decoder.Decode()` on a struct with arrays of other structs could be vulnerable to this memory exhaustion vulnerability. Version 1.4.1 contains a patch for the issue.	7.5	More Details
CVE-2024-38472	SSRF in Apache HTTP Server on Windows allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests or content Users are recommended to upgrade to version 2.4.60 which fixes this issue. Note: Existing configurations that access UNC paths will have to configure new directive "UNCList" to allow access during request processing.	7.5	More Details
CVE-2024-38374	The CycloneDX core module provides a model representation of the SBOM along with utilities to assist in creating, validating, and parsing SBOMs. Before deserializing CycloneDX Bill of Materials in XML format, _cyclonedx-core-java_ leverages XPath expressions to determine the schema version of the BOM. The `DocumentBuilderFactory` used to evaluate XPath expressions was not configured securely, making the library vulnerable to XML External Entity (XXE) injection. This vulnerability has been fixed in cyclonedx-core-java version 9.0.4.	7.5	More Details
CVE-2024-38477	null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. Users are recommended to upgrade to version 2.4.60, which fixes this issue.	7.5	More Details
CVE-2024-39573	Potential SSRF in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to cause unsafe RewriteRules to unexpectedly setup URL's to be handled by mod_proxy. Users are recommended to upgrade to version 2.4.60, which fixes this issue.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39249	Async <= 2.6.4 and <= 3.2.5 are vulnerable to ReDoS (Regular Expression Denial of Service) while parsing function in autoinject function. NOTE: this is disputed by the supplier because there is no realistic threat model: regular expressions are not used with untrusted input.	7.5	More Details
CVE-2024-38528	nptd-rs is a tool for synchronizing your computer's clock, implementing the NTP and NTS protocols. There is a missing limit for accepted NTS-KE connections. This allows an unauthenticated remote attacker to crash ntpd-rs when an NTS-KE server is configured. Non NTS-KE server configurations, such as the default ntpd-rs configuration, are unaffected. This vulnerability has been patched in version 1.1.3.	7.5	More Details
CVE-2024-5598	The Advanced File Manager plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 5.2.4 via the 'fma_local_file_system' function. This makes it possible for unauthenticated attackers to extract sensitive data including backups or other sensitive information if the files have been moved to the built-in Trash folder.	7.5	More Details
CVE-2024-31916	IBM OpenBMC FW1050.00 through FW1050.10 BMCWeb HTTPS server component could disclose sensitive URI content to an unauthorized actor that bypasses authentication channels. IBM X-ForceID: 290026.	7.5	More Details
CVE-2023-38370	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1, under certain configurations, could allow a user on the network to install malicious packages. IBM X-Force ID: 261197.	7.5	More Details
CVE-2024-36991	In Splunk Enterprise on Windows versions below 9.2.2, 9.1.5, and 9.0.10, an attacker could perform a path traversal on the /modules/messaging/ endpoint in Splunk Enterprise on Windows. This vulnerability should only affect Splunk Enterprise on Windows.	7.5	More Details
CVE-2024-36420	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, the `/api/v1/openai-assistants-file` endpoint in `index.ts` is vulnerable to arbitrary file read due to lack of sanitization of the `fileName` body parameter. No known patches for this issue are available.	7.5	More Details
CVE-2024-39130	A NULL Pointer Dereference discovered in DumpTS v0.1.0-nightly allows attackers to cause a denial of service via the function DumpOneStream() at /src/DumpStream.cpp.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38523	Hush Line is a free and open-source, anonymous-tip-line-as-a-service for organizations or individuals. The TOTP authentication flow has multiple issues that weakens its one-time nature. Specifically, the lack of 2FA for changing security settings allows attacker with CSRF or XSS primitives to change such settings without user interaction and credentials are required. This vulnerability has been patched in version 0.10.	7.5	More Details
CVE-2023-52892	In phpseclib before 1.0.22, 2.x before 2.0.46, and 3.x before 3.0.33, some characters in Subject Alternative Name fields in TLS certificates are incorrectly allowed to have a special meaning in regular expressions (such as a + wildcard), leading to name confusion in X.509 certificate host verification.	7.5	More Details
CVE-2024-39348	Download of code without integrity check vulnerability in AirPrint functionality in Synology Router Manager (SRM) before 1.2.5-8227-11 and 1.3.1-9346-8 allows man-in-the-middle attackers to execute arbitrary code via unspecified vectors.	7.5	More Details
CVE-2024-39350	A vulnerability regarding authentication bypass by spoofing is found in the RTSP functionality. This allows man-in-the-middle attackers to obtain privileges without consent via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	7.5	More Details
CVE-2024-5735	Full Path Disclosure vulnerability in AdmirorFrames Joomla! extension in afHelper.php script allows an unauthorised attacker to retrieve location of web root folder. This issue affects AdmirorFrames: before 5.0.	7.5	More Details
CVE-2024-5736	Server Side Request Forgery (SSRF) vulnerability in AdmirorFrames Joomla! extension in afGdStream.php script allows to access local files or server pages available only from localhost. This issue affects AdmirorFrames: before 5.0.	7.5	More Details
CVE-2024-36421	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, A CORS misconfiguration sets the Access-Control-Allow-Origin header to all, allowing arbitrary origins to connect to the website. In the default configuration (unauthenticated), arbitrary origins may be able to make requests to Flowise, stealing information from the user. This CORS misconfiguration may be chained with the path injection to allow an attacker attackers without access to Flowise to read arbitrary files from the Flowise server. As of time of publication, no known patches are available.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31912	IBM MQ 9.3 LTS and 9.3 CD could allow an authenticated user to escalate their privileges under certain configurations due to incorrect privilege assignment. IBM X-Force ID: 289894.	7.5	More Details
CVE-2024-21586	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series and NFX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). If an affected device receives specific valid traffic destined to the device, it will cause the PFE to crash and restart. Continued receipt and processing of this traffic will create a sustained DoS condition. This issue affects Junos OS on SRX Series: * 21.4 versions before 21.4R3-S7.9, * 22.1 versions before 22.1R3-S5.3, * 22.2 versions before 22.2R3-S4.11, * 22.3 versions before 22.3R3, * 22.4 versions before 22.4R3. This issue affects Junos OS on NFX Series: * 21.4 versions before 21.4R3-S8, * 22.1 versions after 22.1R1, * 22.2 versions before 22.2R3-S5, * 22.3 versions before 22.3R3, * 22.4 versions before 22.4R3. Junos OS versions prior to 21.4R1 are not affected by this issue.	7.5	More Details
CVE-2024-36982	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.109 and 9.1.2308.207, an attacker could trigger a null pointer reference on the cluster/config REST endpoint, which could result in a crash of the Splunk daemon.	7.5	More Details
CVE-2024-20077	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01297807; Issue ID: MSV-1482.	7.5	More Details
CVE-2024-3043	An unauthenticated IEEE 802.15.4 'co-ordinator realignment' packet can be used to force Zigbee nodes to change their network identifier (pan ID), leading to a denial of service. This packet type is not useful in production and should be used only for PHY qualification.	7.5	More Details
CVE-2024-20076	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01297806; Issue ID: MSV-1481.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24749	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.23.5 and 2.24.3, if GeoServer is deployed in the Windows operating system using an Apache Tomcat web application server, it is possible to bypass existing input validation in the GeoWebCache ByteStreamController class and read arbitrary classpath resources with specific file name extensions. If GeoServer is also deployed as a web archive using the data directory embedded in the `geoserver.war` file (rather than an external data directory), it will likely be possible to read specific resources to gain administrator privileges. However, it is very unlikely that production environments will be using the embedded data directory since, depending on how GeoServer is deployed, it will be erased and re-installed (which would also reset to the default password) either every time the server restarts or every time a new GeoServer WAR is installed and is therefore difficult to maintain. An external data directory will always be used if GeoServer is running in standalone mode (via an installer or a binary). Versions 2.23.5 and 2.24.3 contain a patch for the issue. Some workarounds are available. One may change from a Windows environment to a Linux environment; or change from Apache Tomcat to Jetty application server. One may also disable anonymous access to the embeded GeoWebCache administration and status pages.	7.5	More Details
CVE-2024-34703	Botan is a C++ cryptography library. X.509 certificates can identify elliptic curves using either an object identifier or using explicit encoding of the parameters. Prior to versions 3.3.0 and 2.19.4, an attacker could present an ECDSA X.509 certificate using explicit encoding where the parameters are very large. The proof of concept used a 16Kbit prime for this purpose. When parsing, the parameter is checked to be prime, causing excessive computation. This was patched in 2.19.4 and 3.3.0 to allow the prime parameter of the elliptic curve to be at most 521 bits. No known workarounds are available. Note that support for explicit encoding of elliptic curve parameters is deprecated in Botan.	7.5	More Details
CVE-2024-24792	Parsing a corrupt or malicious image with invalid color indices can cause a panic.	7.5	More Details
CVE-2024-38525	dd-trace-cpp is the Datadog distributed tracing for C++. When the library fails to extract trace context due to malformed unicode, it logs the list of audited headers and their values using the `nlohmann` JSON library. However, due to the way the JSON library is invoked, it throws an uncaught exception, which results in a crash. This vulnerability has been patched in version 0.2.2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34593	Improper input validation in parsing and distributing RTCP packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability.	7.5	More Details
CVE-2024-36829	Incorrect access control in Teldat M1 v11.00.05.50.01 allows attackers to obtain sensitive information via a crafted query string.	7.5	More Details
CVE-2024-23766	An issue was discovered on HMS Anybus X-Gateway AB7832-F 3 devices. The gateway exposes a web interface on port 80. An unauthenticated GET request to a specific URL triggers the reboot of the Anybus gateway (or at least most of its modules). An attacker can use this feature to carry out a denial of service attack by continuously sending GET requests to that URL.	7.5	More Details
CVE-2022-30636	httpTokenCacheKey uses path.Base to extract the expected HTTP-01 token value to lookup in the DirCache implementation. On Windows, path.Base acts differently to filepath.Base, since Windows uses a different path separator (\ vs. /), allowing a user to provide a relative path, i.e. .well-known/acme-challenge/..\..\asd becomes ..\..\asd. The extracted path is then suffixed with +http-01, joined with the cache directory, and opened. Since the controlled path is suffixed with +http-01 before opening, the impact of this is significantly limited, since it only allows reading arbitrary files on the system if and only if they have this suffix.	7.5	More Details
CVE-2024-34587	Improper input validation in parsing application information from RTCP packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability.	7.5	More Details
CVE-2024-6323	Improper authorization in global search in GitLab EE affecting all versions from 16.11 prior to 16.11.5 and 17.0 prior to 17.0.3 and 17.1 prior to 17.1.1 allows an attacker leak content of a private repository in a public project.	7.5	More Details
CVE-2024-4836	Web services managed by Edito CMS (Content Management System) in versions from 3.5 through 3.25 leak sensitive data as they allow downloading configuration files by an unauthenticated user. The issue in versions 3.5 - 3.25 was removed in releases which dates from 10th of January 2014. Higher versions were never affected.	7.5	More Details
CVE-2024-39894	OpenSSH 9.5 through 9.7 before 9.8 sometimes allows timing attacks against echo-off password entry (e.g., for su and Sudo) because of an ObscureKeystrokeTiming logic error. Similarly, other timing attacks against keystroke entry could occur.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24791	The net/http HTTP/1.1 client mishandled the case where a server responds to a request with an "Expect: 100-continue" header with a non-informational (200 or higher) status. This mishandling could leave a client connection in an invalid state, where the next request sent on the connection will fail. An attacker sending a request to a net/http/httputil.ReverseProxy proxy can exploit this mishandling to cause a denial of service by sending "Expect: 100-continue" requests which elicit a non-informational response from the backend. Each such request leaves the proxy with an invalid connection, and causes one subsequent request using that connection to fail.	7.5	More Details
CVE-2024-39206	An issue discovered in MSP360 Backup Agent v7.8.5.15 and v7.9.4.84 allows attackers to obtain network share credentials used in a backup due to enginesettings.list being encrypted with a hard coded key.	7.5	More Details
CVE-2024-38514	NextChat is a cross-platform ChatGPT/Gemini UI. There is a Server-Side Request Forgery (SSRF) vulnerability due to a lack of validation of the `endpoint` GET parameter on the WebDav API endpoint. This SSRF can be used to perform arbitrary HTTPS request from the vulnerable instance (MKCOL, PUT and GET methods supported), or to target NextChat users and make them execute arbitrary JavaScript code in their browser. This vulnerability has been patched in version 2.12.4.	7.4	More Details
CVE-2024-38994	amoyjs amoy common v1.0.10 was discovered to contain a prototype pollution via the function extend. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	7.3	More Details
CVE-2024-39003	amoyjs amoy common v1.0.10 was discovered to contain a prototype pollution via the function setValue. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	7.3	More Details
CVE-2024-21469	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	7.3	More Details
CVE-2024-34581	The W3C XML Signature Syntax and Processing (XMLDsig) specification, starting with 1.0, was originally published with a "RetrievalMethod is a URI ... that may be used to obtain key and/or certificate information" statement and no accompanying information about SSRF risks, and this may have contributed to vulnerable implementations such as those discussed in CVE-2023-36661 and CVE-2024-21893. NOTE: this was mitigated in 1.1 and 2.0 via a directly referenced Best Practices document that calls on implementers to be wary of SSRF.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6371	A vulnerability, which was classified as critical, has been found in itsourcecode Pool of Bethesda Online Reservation System 1.0. Affected by this issue is some unknown functionality of the file controller.php. The manipulation of the argument rmtype_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-269804.	7.3	More Details
CVE-2024-6418	A vulnerability classified as critical has been found in SourceCodester Medicine Tracker System 1.0. This affects an unknown part of the file /classes/Users.php?f=register_user. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-270009 was assigned to this vulnerability.	7.3	More Details
CVE-2024-6373	A vulnerability has been found in itsourcecode Online Food Ordering System up to 1.0 and classified as critical. This vulnerability affects unknown code of the file /addproduct.php. The manipulation of the argument photo leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-269806 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-39373	TELSAT marKoni FM Transmitters are vulnerable to a command injection vulnerability through the manipulation of settings and could allow an attacker to gain unauthorized access to the system with administrative privileges.	7.2	More Details
CVE-2024-36074	Netwrix CoSoSys Endpoint Protector through 5.9.3 and CoSoSys Unify through 7.0.6 contain a remote code execution vulnerability in the Endpoint Protector and Unify agent in the way that the EasyLock dependency is acquired from the server. An attacker with administrative access to the Endpoint Protector or Unify server can cause a client to acquire and execute a malicious file resulting in remote code execution.	7.2	More Details
CVE-2023-41922	A 'Cross-site Scripting' (XSS) vulnerability, characterized by improper input neutralization during web page generation, has been discovered. This vulnerability allows for Stored XSS attacks to occur. Multiple areas within the administration interface of the webserver lack adequate input validation, resulting in multiple instances of Stored XSS vulnerabilities.	7.2	More Details
CVE-2024-36073	Netwrix CoSoSys Endpoint Protector through 5.9.3 and CoSoSys Unify through 7.0.6 contain a remote code execution vulnerability in the shadowing component of the Endpoint Protector and Unify agent which allows an attacker with administrative access to the Endpoint Protector or Unify server to overwrite sensitive configuration and subsequently execute system commands with SYSTEM/root privileges on a chosen client endpoint.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47802	A vulnerability regarding improper neutralization of special elements used in an OS command ('OS Command Injection') is found in the IP block functionality. This allows remote authenticated users with administrator privileges to execute arbitrary commands via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	7.2	More Details
CVE-2024-4869	The WP Cookie Consent (for GDPR, CCPA & ePrivacy) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘Client-IP’ header in all versions up to, and including, 3.2.0 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-2024-38526	pdoc provides API Documentation for Python Projects. Documentation generated with `pdoc --math` linked to JavaScript files from polyfill.io. The polyfill.io CDN has been sold and now serves malicious code. This issue has been fixed in pdoc 14.5.1.	7.2	More Details
CVE-2024-3123	CHANGING Mobile One Time Password's uploading function in a hidden page does not filter file type properly. Remote attackers with administrator privilege can exploit this vulnerability to upload and run malicious file to execute system commands.	7.2	More Details
CVE-2024-39351	A vulnerability regarding improper neutralization of special elements used in an OS command ('OS Command Injection') is found in the NTP configuration. This allows remote authenticated users with administrator privileges to execute arbitrary commands via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	7.2	More Details
CVE-2023-41923	The user management section of the web application permits the creation of user accounts with excessively weak passwords, including single-character passwords.	7.2	More Details
CVE-2024-28798	IBM InfoSphere Information Server 11.7 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 287172.	7.2	More Details
CVE-2024-21462	Transient DOS while loading the TA ELF file.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36989	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200, a low-privileged user that does not hold the admin or power Splunk roles could create notifications in Splunk Web Bulletin Messages that all users on the instance receive.	7.1	More Details
CVE-2024-21460	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space.	7.1	More Details
CVE-2024-39323	aimeos/ai-admin-graphql is the Aimeos GraphQL API admin interface. Starting in version 2022.04.01 and prior to versions 2022.10.10, 2023.10.6, and 2024.04.6, an improper access control vulnerability allows an editor to modify and take over an admin account in the back end. Versions 2022.10.10, 2023.10.6, and 2024.04.6 fix this issue.	7.1	More Details
CVE-2024-38532	The NXP Data Co-Processor (DCP) is a built-in hardware module for specific NXP SoCs[1] that implements a dedicated AES cryptographic engine for encryption/decryption operations. The dcp_tool reference implementation included in the repository selected the test key, regardless of its `-t` argument. This issue has been patched in commit 26a7.	7.1	More Details
CVE-2024-28982	Hitachi Vantara Pentaho Business Analytics Server versions before 10.1.0.0 and 9.3.0.7, including 8.3.x do not correctly protect the ACL service endpoint of the Pentaho User Console against XML External Entity Reference.	7.1	More Details
CVE-2024-6376	MongoDB Compass may be susceptible to code injection due to insufficient sandbox protection settings with the usage of ejson shell parser in Compass' connection handling. This issue affects MongoDB Compass versions prior to version 1.42.2	7.0	More Details
CVE-2024-39708	An issue was discovered in the Agent in Delinea Privilege Manager (formerly Thycotic Privilege Manager) before 12.0.1096 on Windows. Sometimes, a non-administrator user can copy a crafted DLL file to a temporary directory (used by .NET Shadow Copies) such that privilege escalation can occur if the core agent service loads that file.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3331	Vulnerability in Spotfire Spotfire Enterprise Runtime for R - Server Edition, Spotfire Spotfire Statistics Services, Spotfire Spotfire Analyst, Spotfire Spotfire Desktop, Spotfire Spotfire Server allows The impact of this vulnerability depends on the privileges of the user running the affected software..This issue affects Spotfire Enterprise Runtime for R - Server Edition: from 1.12.7 through 1.20.0; Spotfire Statistics Services: from 12.0.7 through 12.3.1, from 14.0.0 through 14.3.0; Spotfire Analyst: from 12.0.9 through 12.5.0, from 14.0.0 through 14.3.0; Spotfire Desktop: from 14.0 through 14.3.0; Spotfire Server: from 12.0.10 through 12.5.0, from 14.0.0 through 14.3.0.	6.8	More Details
CVE-2024-32757	Under certain circumstances unnecessary user details are provided within system logs	6.8	More Details
CVE-2024-29173	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain a Server-Side Request Forgery (SSRF) vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to disclosure of information on the application or remote client.	6.8	More Details
CVE-2024-32932	Under certain circumstances the web interface users credentials may be recovered by an authenticated user.	6.8	More Details
CVE-2024-32756	Under certain circumstances the Linux users credentials may be recovered by an authenticated user.	6.8	More Details
CVE-2024-36755	D-Link DIR-1950 up to v1.11B03 does not validate SSL certificates when requesting the latest firmware version and downloading URL. This can allow attackers to downgrade the firmware version or change the downloading URL via a man-in-the-middle attack.	6.8	More Details
CVE-2024-39428	In trusty 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	6.8	More Details
CVE-2024-22260	VMware Workspace One UEM update addresses an information exposure vulnerability. A malicious actor with network access to the Workspace One UEM may be able to perform an attack resulting in an information exposure.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5430	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.10 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows a project maintainer can delete the merge request approval policy via graphQL.	6.8	More Details
CVE-2024-39155	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/ipRecord_deal.php?mudi=add.	6.8	More Details
CVE-2024-21482	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image.	6.8	More Details
CVE-2024-5714	In lunary-ai/lunary version 1.2.4, an improper access control vulnerability allows members with team management permissions to manipulate project identifiers in requests, enabling them to invite users to projects in other organizations, change members to projects in other organizations with escalated privileges, and change members from other organizations to their own or other projects, also with escalated privileges. This vulnerability is due to the backend's failure to validate project identifiers against the current user's organization ID and projects belonging to it, as well as a misconfiguration in attribute naming (`org_id` should be `orgId`) that prevents proper user organization validation. As a result, attackers can cause inconsistencies on the platform for affected users and organizations, including unauthorized privilege escalation. The issue is present in the backend API endpoints for user invitation and modification, specifically in the handling of project IDs in requests.	6.8	More Details
CVE-2024-37132	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an incorrect privilege assignment vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of service and Elevation of privileges.	6.7	More Details
CVE-2024-37133	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to unauthorized gain of root-level access.	6.7	More Details
CVE-2024-37126	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to unauthorized gain of root-level access.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37134	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability to gain root-level access.	6.7	More Details
CVE-2024-32854	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privilege attacker could potentially exploit this vulnerability, leading to privilege escalation.	6.7	More Details
CVE-2024-32228	FFmpeg 7.0 is vulnerable to Buffer Overflow. There is a SEGV at libavcodec/hevcdec.c:2947:22 in hevc_frame_end.	6.6	More Details
CVE-2024-5071	The Bookster WordPress plugin through 1.1.0 allows adding sensitive parameters when validating appointments allowing attackers to manipulate the data sent when booking an appointment (the request body) to change its status from pending to approved.	6.5	More Details
CVE-2024-39853	adolph_dudu ratio-swiper 0.0.2 was discovered to contain a prototype pollution via the function parse. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	6.5	More Details
CVE-2024-5570	The Simple Photoswipe WordPress plugin through 0.1 does not have authorisation check when updating its settings, which could allow any authenticated users, such as subscriber to update them	6.5	More Details
CVE-2024-35155	IBM MQ Console 9.3 LTS and 9.3 CD could disclose could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 292765.	6.5	More Details
CVE-2024-39316	Rack is a modular Ruby web server interface. Starting in version 3.1.0 and prior to version 3.1.5, Regular Expression Denial of Service (ReDoS) vulnerability exists in the `Rack::Request::Helpers` module when parsing HTTP Accept headers. This vulnerability can be exploited by an attacker sending specially crafted `Accept-Encoding` or `Accept-Language` headers, causing the server to spend excessive time processing the request and leading to a Denial of Service (DoS). The fix for CVE-2024-26146 was not applied to the main branch and thus while the issue was fixed for the Rack v3.0 release series, it was not fixed in the v3.1 release series until v3.1.5. Users of versions on the 3.1 branch should upgrade to version 3.1.5 to receive the fix.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6402	A vulnerability classified as critical was found in Tenda A301 15.13.08.12. Affected by this vulnerability is the function fromSetWirelessRepeat of the file /goform/SetOnlineDevName. The manipulation of the argument devName leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-269947. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.5	More Details
CVE-2024-6403	A vulnerability, which was classified as critical, has been found in Tenda A301 15.13.08.12. Affected by this issue is the function formWifiBasicSet of the file /goform/SetOnlineDevName. The manipulation of the argument devName leads to stack-based buffer overflow. 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-269948. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.5	More Details
CVE-2024-39000	adolph_dudu ratio-swiper v0.0.2 was discovered to contain a prototype pollution via the function parse. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	6.5	More Details
CVE-2024-37139	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain an Improper Control of a Resource Through its Lifetime vulnerability in an admin operation. A remote low privileged attacker could potentially exploit this vulnerability, leading to temporary resource constraint of system application. Exploitation may lead to denial of service of the application.	6.5	More Details
CVE-2024-38997	adolph_dudu ratio-swiper v0.0.2 was discovered to contain a prototype pollution via the function extendDefaults. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	6.5	More Details
CVE-2024-21458	Information disclosure while handling SA query action frame.	6.5	More Details
CVE-2024-20892	Improper verification of signature in FilterProvider prior to SMR Jul-2024 Release 1 allows local attackers to execute privileged behaviors. User interaction is required for triggering this vulnerability.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37247	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in twinpictures, baden03 jQuery T(-) Countdown Widget allows Stored XSS.This issue affects jQuery T(-) Countdown Widget: from n/a through 2.3.25.	6.5	More Details
CVE-2024-39305	Envoy is a cloud-native, open source edge and service proxy. Prior to versions 1.30.4, 1.29.7, 1.28.5, and 1.27.7. Envoy references already freed memory when route hash policy is configured with cookie attributes. Note that this vulnerability has been fixed in the open as the effect would be immediately apparent if it was configured. Memory allocated for holding attribute values is freed after configuration was parsed. During request processing Envoy will attempt to copy content of de-allocated memory into request cookie header. This can lead to arbitrary content of Envoy's memory to be sent to the upstream service or abnormal process termination. This vulnerability is fixed in Envoy versions v1.30.4, v1.29.7, v1.28.5, and v1.27.7. As a workaround, do not use cookie attributes in route action hash policy.	6.5	More Details
CVE-2024-39313	toy-blog is a headless content management system implementation. Starting in version 0.5.4 and prior to version 0.6.1, articles with private visibility can be read if the reader does not set credentials for the request. Users should upgrade to 0.6.1 or later to receive a patch. No known workarounds are available.	6.5	More Details
CVE-2024-38533	ZKsync Era is a layer 2 rollup that uses zero-knowledge proofs to scale Ethereum. There is possible invalid stack access due to the addresses used to access the stack not properly being converted to cells. This issue has been patched in version 1.5.0.	6.5	More Details
CVE-2024-36990	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.2.2403.100, an authenticated, low-privileged user that does not hold the admin or power Splunk roles could send a specially crafted HTTP POST request to the datamodel/web REST endpoint in Splunk Enterprise, potentially causing a denial of service.	6.5	More Details
CVE-2024-35156	IBM MQ 9.3 LTS and 9.3 CD could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 292766.	6.5	More Details
CVE-2024-3017	In a Silicon Labs multi-protocol gateway, a corrupt pointer to buffered data on a multi-protocol radio co-processor (RCP) causes the OpenThread Border Router(OTBR) application task running on the host platform to crash, allowing an attacker to cause a temporary denial-of-service.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4557	Multiple Denial of Service (DoS) conditions has been discovered in GitLab CE/EE affecting all versions starting from 1.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1 which allowed an attacker to cause resource exhaustion via banzai pipeline.	6.5	More Details
CVE-2024-3959	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.7 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows private job artifacts can be accessed by any user.	6.5	More Details
CVE-2024-5642	CPython 3.9 and earlier doesn't disallow configuring an empty list ("[]") for SSLContext.set_npn_protocols() which is an invalid value for the underlying OpenSSL API. This results in a buffer over-read when NPN is used (see CVE-2024-5535 for OpenSSL). This vulnerability is of low severity due to NPN being not widely used and specifying an empty list likely being uncommon in-practice (typically a protocol name would be configured).	6.5	More Details
CVE-2024-37248	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Anima allows Stored XSS.This issue affects Anima: from n/a through 1.4.1.	6.5	More Details
CVE-2024-1493	An issue was discovered in GitLab CE/EE affecting all versions starting from 9.2 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, with the processing logic for generating link in dependency files can lead to a regular expression DoS attack on the server	6.5	More Details
CVE-2024-21466	Information disclosure while parsing sub-IE length during new IE generation.	6.5	More Details
CVE-2024-21457	INformation disclosure while handling Multi-link IE in beacon frame.	6.5	More Details
CVE-2024-38950	Heap Buffer Overflow vulnerability in Libde265 v1.0.15 allows attackers to crash the application via crafted payload to __interceptor_memcpy function.	6.5	More Details
CVE-2024-21456	Information Disclosure while parsing beacon frame in STA.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38949	Heap Buffer Overflow vulnerability in Libde265 v1.0.15 allows attackers to crash the application via crafted payload to display444as420 function at sdl.cc	6.5	More Details
CVE-2024-36075	The CoSoSys Endpoint Protector through 5.9.3 and Unify agent through 7.0.6 is susceptible to an arbitrary code execution vulnerability due to the way an archive obtained from the Endpoint Protector or Unify server is extracted on the endpoint. An attacker who is able to modify the archive on the server could obtain remote code execution as an administrator on an endpoint.	6.5	More Details
CVE-2024-39132	A NULL Pointer Dereference vulnerability in DumpTS v0.1.0-nightly allows attackers to cause a denial of service via the function VerifyCommandLine() at /src/DumpTS.cpp.	6.5	More Details
CVE-2024-25031	IBM Storage Defender - Resiliency Service 2.0.0 through 2.0.4 uses an inadequate account lockout setting that could allow an attacker on the network to brute force account credentials. IBM X-Force ID: 281678.	6.5	More Details
CVE-2024-5173	The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Video player widget settings in all versions up to, and including, 2.5.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5819	The Gutenberg Blocks with AI by Kadence WP – Page Builder Features plugin for WordPress is vulnerable to DOM-based Stored Cross-Site Scripting via HTML data attributes in all versions up to, and including, 3.2.45 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-28797	IBM InfoSphere Information Server 11.7 is vulnerable stored to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 287136.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5790	The Happy Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘url’ attribute within the plugin's Gradient Heading widget in all versions up to, and including, 3.11.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5666	The Extensions for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘url’ parameter within the EE Button widget in all versions up to, and including, 2.0.30 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5192	The Funnel Builder for WordPress by FunnelKit – Customize WooCommerce Checkout Pages, Create Sales Funnels, Order Bumps & One Click Upsells plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘mimes’ parameter in all versions up to, and including, 3.3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-6382	Incorrect handling of certain string inputs may result in MongoDB Rust driver constructing unintended server commands. This may cause unexpected application behavior including data modification. This issue affects MongoDB Rust Driver 2.0 versions prior to 2.8.2	6.4	More Details
CVE-2024-5332	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Card widget in all versions up to, and including, 2.6.9.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4268	The Ultimate Blocks – WordPress Blocks Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's blocks in all versions up to, and including, 3.1.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5925	The Theron Lite theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘url’ parameter within the theme's Button shortcode in all versions up to, and including, 2.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5922	The Scylla lite theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘url’ parameter within the theme's Button shortcode in all versions up to, and including, 1.8.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5938	The Boot Store theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘link’ parameter within the theme's Button shortcode in all versions up to, and including, 1.6.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5419	The Void Contact Form 7 Widget For Elementor Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cf7_redirect_page' attribute within the plugin's Void Contact From 7 widget in all versions up to, and including, 2.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-6262	The Portfolio Gallery – Image Gallery Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'PFG' shortcode in all versions up to, and including, 1.6.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4983	The The Plus Addons for Elementor – Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'video_color' parameter in all versions up to, and including, 5.6.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5601	The Create by Mediavine plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Schema Meta shortcode in all versions up to, and including, 1.9.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1427	The The Post Grid – Shortcode, Gutenberg Blocks and Elementor Addon for Post Grid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the section title tag attribute in all versions up to, and including, 7.7.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5219	The Easy Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file upload feature in all versions up to, and including, 1.11.15 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4570	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in versions up to, and including, 1.13.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4569	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘url’ parameter in versions up to, and including, 1.13.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5289	The Gutenberg Blocks with AI by Kadence WP – Page Builder Features plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Google Maps widget parameters in all versions up to, and including, 3.2.42 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3513	The Ultimate Blocks – WordPress Blocks Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the title tag parameter in all versions up to, and including, 3.1.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5504	The Rife Elementor Extensions & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tag' attribute within the plugin's Writing Effect Headline widget in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5260	The Sina Extension for Elementor (Slider, Gallery, Form, Modal, Data Table, Tab, Particle, Free Elementor Widgets & Elementor Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘read_more_text’ parameter in all versions up to, and including, 3.5.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6296	The Stackable – Page Builder Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘data-caption’ parameter in all versions up to, and including, 3.13.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-6264	The Post Meta Data Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘$meta_key’ parameter in all versions up to, and including, 1.2.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5215	The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 2.5.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5788	The Silesia theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘link’ attribute within the theme's Button shortcode in all versions up to, and including, 1.0.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5662	The Ultimate Post Kit Addons For Elementor – (Post Grid, Post Carousel, Post Slider, Category List, Post Tabs, Timeline, Post Ticker, Tag Cloud) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘url’ parameter within the Social Count (Static) widget in all versions up to, and including, 3.11.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5424	The Gallery Blocks with Lightbox. Image Gallery, (HTML5 video , YouTube, Vimeo) Video Gallery and Lightbox for native gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘galleryID’ and 'className' parameters in all versions up to, and including, 3.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5796	The Infinite theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘project_url’ parameter in all versions up to, and including, 1.1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-6363	The Stock Ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's stock_ticker shortcode in all versions up to, and including, 3.24.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-38990	Tada5hi sp-common v0.5.4 was discovered to contain a prototype pollution via the function mergeDeep. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	6.3	More Details
CVE-2024-6452	A vulnerability classified as critical was found in linlinjava litemall up to 1.8.0. Affected by this vulnerability is an unknown functionality of the file AdminGoodscontroller.java. The manipulation of the argument goodsId/goodsSn/name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-270235.	6.3	More Details
CVE-2024-38987	aofl cli-lib v3.14.0 was discovered to contain a prototype pollution via the component defaultsDeep. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6441	A vulnerability was found in ORIPA up to 1.72. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file src/main/java/oripa/persistence/doc/loader/LoaderXML.java. The manipulation leads to deserialization. The attack can be launched remotely. Upgrading to version 1.80 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-270169 was assigned to this vulnerability.	6.3	More Details
CVE-2024-39002	rjrodger jsonic-next v2.12.1 was discovered to contain a prototype pollution via the function util.clone. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	6.3	More Details
CVE-2024-6440	A vulnerability was found in SourceCodester Home Owners Collection Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /classes/Master.php?f=delete_category. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-270168.	6.3	More Details
CVE-2024-36986	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, an authenticated user could run risky commands using the permissions of a higher-privileged user to bypass SPL safeguards for risky commands in the Analytics Workspace. The vulnerability requires the authenticated user to phish the victim by tricking them into initiating a request within their browser. The authenticated user should not be able to exploit the vulnerability at will.	6.3	More Details
CVE-2024-6416	A vulnerability was found in SeaCMS 12.9. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /js/player/dmplayer/dmku/?ac=edit. The manipulation of the argument cid with the input (select(0)from(select(sleep(10)))v) leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-270007.	6.3	More Details
CVE-2024-6417	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/ajax.php?action=delete_user. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-270008.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6439	A vulnerability was found in SourceCodester Home Owners Collection Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /classes/Users.php?f=save. The manipulation of the argument img 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-270167.	6.3	More Details
CVE-2024-6419	A vulnerability classified as critical was found in SourceCodester Medicine Tracker System 1.0. This vulnerability affects unknown code of the file /classes/Master.php?f=save_medicine. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-270010 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-39018	harvey-woo cat5th/key-serializer v0.2.5 was discovered to contain a prototype pollution via the function "query". This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	6.3	More Details
CVE-2024-39001	ag-grid-enterprise v31.3.2 was discovered to contain a prototype pollution via the component _ModuleSupport.jsonApply. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	6.3	More Details
CVE-2024-6438	A vulnerability has been found in Hitout Carsale 1.0 and classified as critical. This vulnerability affects unknown code of the file OrderController.java. The manipulation of the argument orderBy leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-270166 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-6453	A vulnerability was found in itsourcecode Farm Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /quarantine.php?id=3. The manipulation of the argument pigno/breed/reason 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-270241 was assigned to this vulnerability. NOTE: Original submission mentioned parameter pigno only but the VulDB data analysis team determined two additional parameters to be affected as well.	6.3	More Details
CVE-2023-26877	File upload vulnerability found in Softexpert Excellence Suite v.2.1 allows attackers to execute arbitrary code via a .php file upload to the form/efms_exec_html/file_upload_parser.php endpoint.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6372	A vulnerability, which was classified as critical, was found in itsourcecode Tailoring Management System 1.0. This affects an unknown part of the file customeradd.php. The manipulation of the argument fullname/address/phonenumber/sex/email/city/comment 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-269805 was assigned to this vulnerability.	6.3	More Details
CVE-2024-39209	luci-app-sms-tool v1.9-6 was discovered to contain a command injection vulnerability via the score parameter.	6.3	More Details
CVE-2024-31802	DESIGNA ABACUS v.18 and before allows an attacker to bypass the payment process via a crafted QR code.	6.3	More Details
CVE-2024-28820	Buffer overflow in the extract_openvpn_cr function in openvpn-cr.c in openvpn-auth-ldap (aka the Three Rings Auth-LDAP plugin for OpenVPN) 2.0.4 allows attackers with a valid LDAP username and who can control the challenge/response password field to pass a string with more than 14 colons into this field and cause a buffer overflow.	6.3	More Details
CVE-2024-38522	Hush Line is a free and open-source, anonymous-tip-line-as-a-service for organizations or individuals. The CSP policy applied on the `tips.hushline.app` website and bundled by default in this repository is trivial to bypass. This vulnerability has been patched in version 0.1.0.	6.3	More Details
CVE-2024-35139	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could allow a local user to obtain sensitive information from the container due to incorrect default permissions. IBM X-Force ID: 292415.	6.2	More Details
CVE-2024-35137	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could allow a local user to possibly elevate their privileges due to sensitive configuration information being exposed. IBM X-Force ID: 292413.	6.2	More Details
CVE-2024-33326	A cross-site scripting (XSS) vulnerability in the component XsltResultControllerHtml.jsp of Lumisxp v15.0.x to v16.1.x allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the lumPageID parameter.	6.1	More Details
CVE-2024-35545	MAP-OS v4.45.0 and earlier was discovered to contain a cross-site scripting (XSS) vulnerability.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3801	Sites managed in S@M CMS (Concept Intermedia) might be vulnerable to Reflected XSS via including scripts in one of GET header parameters. Only a part of observed services is vulnerable, but since vendor has not investigated the root problem, it is hard to determine when the issue appears.	6.1	More Details
CVE-2024-3800	Sites managed in S@M CMS (Concept Intermedia) might be vulnerable to Reflected XSS via including scripts in requested file names. Only a part of observed services is vulnerable, but since vendor has not investigated the root problem, it is hard to determine when the issue appears.	6.1	More Details
CVE-2024-5737	Script afGdStream.php in AdmirorFrames Joomla! extension doesn't specify a content type and as a result default (text/html) is used. An attacker may embed HTML tags directly in image data which is rendered by a webpage as HTML. This issue affects AdmirorFrames: before 5.0.	6.1	More Details
CVE-2024-5730	The Pagerank tools WordPress plugin through 1.1.5 does not sanitise and escape a parameter 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-2024-5729	The Simple AL Slider WordPress plugin through 1.2.10 does not sanitise and escape a parameter 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-2024-5544	The Media Library Assistant plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the order parameter in all versions up to, and including, 3.17 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-38953	phpok 6.4.003 contains a Cross Site Scripting (XSS) vulnerability in the ok_f() method under the framework/api/upload_control.php file.	6.1	More Details
CVE-2024-6050	Improper Neutralization of Input During Web Page Generation vulnerability in SOKRATES-software SOWA OPAC allows a Reflected Cross-Site Scripting (XSS). An attacker might trick somebody into using a crafted URL, which will cause a script to be run in user's browser. This issue affects SOWA OPAC software in versions from 4.0 before 4.9.10, from 5.0 before 6.2.12.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39241	Cross Site Scripting (XSS) vulnerability in skycaiji 2.8 allows attackers to run arbitrary code via /admin/tool/preview.	6.1	More Details
CVE-2024-36422	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, a reflected cross-site scripting vulnerability occurs in the `api/v1/chatflows/id` endpoint. If the default configuration is used (unauthenticated), an attacker may be able to craft a specially crafted URL that injects Javascript into the user sessions, allowing the attacker to steal information, create false popups, or even redirect the user to other websites without interaction. If the chatflow ID is not found, its value is reflected in the 404 page, which has type text/html. This allows an attacker to attach arbitrary scripts to the page, allowing an attacker to steal sensitive information. This XSS may be chained with the path injection to allow an attacker without direct access to Flowise to read arbitrary files from the Flowise server. As of time of publication, no known patches are available.	6.1	More Details
CVE-2024-21520	Versions of the package djangorestframework before 3.15.2 are vulnerable to Cross-site Scripting (XSS) via the break_long_headers template filter due to improper input sanitization before splitting and joining with tags.	6.1	More Details
CVE-2024-37145	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, a reflected cross-site scripting vulnerability occurs in the `/api/v1/chatflows-streaming/id` endpoint. If the default configuration is used (unauthenticated), an attacker may be able to craft a specially crafted URL that injects Javascript into the user sessions, allowing the attacker to steal information, create false popups, or even redirect the user to other websites without interaction. If the chatflow ID is not found, its value is reflected in the 404 page, which has type text/html. This allows an attacker to attach arbitrary scripts to the page, allowing an attacker to steal sensitive information. This XSS may be chained with the path injection to allow an attacker without direct access to Flowise to read arbitrary files from the Flowise server. As of time of publication, no known patches are available.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37146	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, a reflected cross-site scripting vulnerability occurs in the `/api/v1/credentials/id` endpoint. If the default configuration is used (unauthenticated), an attacker may be able to craft a specially crafted URL that injects Javascript into the user sessions, allowing the attacker to steal information, create false popups, or even redirect the user to other websites without interaction. If the chatflow ID is not found, its value is reflected in the 404 page, which has type text/html. This allows an attacker to attach arbitrary scripts to the page, allowing an attacker to steal sensitive information. This XSS may be chained with the path injection to allow an attacker without direct access to Flowise to read arbitrary files from the Flowise server. As of time of publication, no known patches are available.	6.1	More Details
CVE-2024-39242	A cross-site scripting (XSS) vulnerability in skycaiji v2.8 allows attackers to execute arbitrary web scripts or HTML via a crafted payload using eval(String.fromCharCode()).	6.1	More Details
CVE-2024-33327	A cross-site scripting (XSS) vulnerability in the component UrlAccessibilityEvaluation.jsp of Lumisxp v15.0.x to v16.1.x allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the contentHtml parameter.	6.1	More Details
CVE-2024-20893	Improper input validation in libmediaextractorservice.so prior to SMR Jul-2024 Release 1 allows local attackers to trigger memory corruption.	6.1	More Details
CVE-2024-4704	The Contact Form 7 WordPress plugin before 5.9.5 has an open redirect that allows an attacker to utilize a false URL and redirect to the URL of their choosing.	6.1	More Details
CVE-2024-36423	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, a reflected cross-site scripting vulnerability occurs in the `/api/v1/public-chatflows/id` endpoint. If the default configuration is used (unauthenticated), an attacker may be able to craft a specially crafted URL that injects Javascript into the user sessions, allowing the attacker to steal information, create false popups, or even redirect the user to other websites without interaction. If the chatflow ID is not found, its value is reflected in the 404 page, which has type text/html. This allows an attacker to attach arbitrary scripts to the page, allowing an attacker to steal sensitive information. This XSS may be chained with the path injection to allow an attacker without direct access to Flowise to read arbitrary files from the Flowise server. As of time of publication, no known patches are available.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4604	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Magarsus Consultancy SSO (Single Sign On) allows Manipulating Hidden Fields.This issue affects SSO (Single Sign On): from 1.0 before 1.1.	6.1	More Details
CVE-2024-6405	The Floating Social Buttons plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5. This is due to missing or incorrect nonce validation on the floating_social_buttons_option() function. This makes it possible for unauthenticated attackers to update the plugins settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-5062	A reflected Cross-Site Scripting (XSS) vulnerability was identified in zenml-io/zenml version 0.57.1. The vulnerability exists due to improper neutralization of input during web page generation, specifically within the survey redirect parameter. This flaw allows an attacker to redirect users to a specified URL after completing a survey, without proper validation of the 'redirect' parameter. Consequently, an attacker can execute arbitrary JavaScript code in the context of the user's browser session. This vulnerability could be exploited to steal cookies, potentially leading to account takeover.	6.1	More Details
CVE-2024-39828	R74n Sandboxels 1.9 through 1.9.5 allows XSS via a message in a modified saved-game file. This was fixed in a hotfix to 1.9.5 on 2024-06-29.	6.1	More Details
CVE-2023-4017	The Goya theme for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘attra-color’, 'attra-size', and 'product-cata' parameters in versions up to, and including, 1.0.8.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-5889	The Events Manager – Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘country’ parameter in all versions up to, and including, 6.4.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20399	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated user in possession of Administrator credentials to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials. The following Cisco devices already allow administrative users to access the underlying operating system through the bash-shell feature, so, for these devices, this vulnerability does not grant any additional privileges: Nexus 3000 Series Switches Nexus 7000 Series Switches that are running Cisco NX-OS Software releases 8.1(1) and later Nexus 9000 Series Switches in standalone NX-OS mode	6.0	More Details
CVE-2024-34586	Improper access control in KnoxCustomManagerService prior to SMR Jul-2024 Release 1 allows local attackers to configure Knox privacy policy.	5.9	More Details
CVE-2024-39347	Incorrect default permissions vulnerability in firewall functionality in Synology Router Manager (SRM) before 1.2.5-8227-11 and 1.3.1-9346-8 allows man-in-the-middle attackers to access highly sensitive intranet resources via unspecified vectors.	5.9	More Details
CVE-2024-29175	Dell PowerProtect Data Domain, versions prior to 7.13.0.0, LTS 7.7.5.40, LTS 7.10.1.30 contain an weak cryptographic algorithm vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to man-in-the-middle attack that exposes sensitive session information.	5.9	More Details
CVE-2024-20901	Improper input validation in copying data to buffer cache in libsaped prior to SMR Jul-2024 Release 1 allows local attackers to write out-of-bounds memory.	5.9	More Details
CVE-2024-25053	IBM Cognos Analytics 11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 12.0.0, 12.0.1, and 12.0.2 is vulnerable to improper certificate validation when using the IBM Planning Analytics Data Source Connection. This could allow an attacker to spoof a trusted entity by interfering in the communication path between IBM Planning Analytics server and IBM Cognos Analytics server. IBM X-Force ID: 283364.	5.9	More Details
CVE-2024-20889	Improper authentication in BLE prior to SMR Jul-2024 Release 1 allows adjacent attackers to pair with devices.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5573	The Easy Table of Contents WordPress plugin before 2.0.66 does not sanitise and escape some of its settings, which could allow high privilege users such as editors to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	5.9	More Details
CVE-2024-32852	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.0 contain use of a broken or risky cryptographic algorithm vulnerability. An unprivileged network malicious attacker could potentially exploit this vulnerability, leading to data leaks.	5.9	More Details
CVE-2024-28973	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain a Stored Cross-Site Scripting Vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to the storage of malicious HTML or JavaScript codes in a trusted application data store. When a high privileged victim user accesses the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery	5.9	More Details
CVE-2024-6388	Marco Trevisan discovered that the Ubuntu Advantage Desktop Daemon, before version 1.12, leaks the Pro token to unprivileged users by passing the token as an argument in plaintext.	5.9	More Details
CVE-2023-38371	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 261198.	5.9	More Details
CVE-2024-34601	Improper verification of intent by broadcast receiver vulnerability in GalaxyStore prior to version 4.5.81.0 allows local attackers to launch unexported activities of GalaxyStore.	5.9	More Details
CVE-2024-29954	A vulnerability in a password management API in Brocade Fabric OS versions before v9.2.1, v9.2.0b, v9.1.1d, and v8.2.3e prints sensitive information in log files. This could allow an authenticated user to view the server passwords for protocols such as scp and sftp. Detail. When the firmwaredownload command is incorrectly entered or points to an erroneous file, the firmware download log captures the failed command, including any password entered in the command line.	5.9	More Details
CVE-2024-35116	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, and 9.3 CD is vulnerable to a denial of service attack caused by an error applying configuration changes. IBM X-Force ID: 290335.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34596	Improper authentication in SmartThings prior to version 1.8.17 allows remote attackers to bypass the expiration date for members set by the owner.	5.9	More Details
CVE-2024-31919	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS and 9.3 CD, in certain configurations, is vulnerable to a denial of service attack caused by an error processing messages when an API Exit using MQBUFMH is used. IBM X-Force ID: 290259.	5.9	More Details
CVE-2024-4105	A vulnerability has been found in FAST/TOOLS and CI Server. The affected product's WEB HMI server's function to process HTTP requests has a security flaw (Reflected XSS) that allows the execution of malicious scripts. Therefore, if a client PC with inadequate security measures accesses a product URL containing a malicious request, the malicious script may be executed on the client PC. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04 CI Server R1.01.00 to R1.03.00	5.8	More Details
CVE-2024-39315	Pomerium is an identity and context-aware access proxy. Prior to version 0.26.1, the Pomerium user info page (at `/.pomerium`) unintentionally included serialized OAuth2 access and ID tokens from the logged-in user's session. These tokens are not intended to be exposed to end users. This issue may be more severe in the presence of a cross-site scripting vulnerability in an upstream application proxied through Pomerium. If an attacker could insert a malicious script onto a web page proxied through Pomerium, that script could access these tokens by making a request to the `/.pomerium` endpoint. Upstream applications that authenticate only the ID token may be vulnerable to user impersonation using a token obtained in this manner. Note that an OAuth2 access token or ID token by itself is not sufficient to hijack a user's Pomerium session. Upstream applications should not be vulnerable to user impersonation via these tokens provided the application verifies the Pomerium JWT for each request, the connection between Pomerium and the application is secured by mTLS, or the connection between Pomerium and the application is otherwise secured at the network layer. The issue is patched in Pomerium v0.26.1. No known workarounds are available.	5.7	More Details
CVE-2023-38368	IBM Security Access Manager Docker 10.0.0.0 through 10.0.7.1 could disclose sensitive information to a local user to do improper permission controls. IBM X-Force ID: 261195.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30430	IBM Security Verify Access 10.0.0 through 10.0.7.1 could allow a local user to obtain sensitive information from trace logs. IBM X-Force ID: 252183.	5.5	More Details
CVE-2022-25479	Vulnerability in Realtek RtsPer driver for PCIe Card Reader (RtsPer.sys) before 10.0.22000.21355 and Realtek RtsUer driver for USB Card Reader (RtsUer.sys) before 10.0.22000.31274 allows for the leakage of kernel memory from both the stack and the heap.	5.5	More Details
CVE-2024-34594	Exposure of sensitive information in proc file system prior to SMR Jul-2024 Release 1 allows local attackers to read kernel memory address.	5.5	More Details
CVE-2023-51777	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error.	5.5	More Details
CVE-2024-22102	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error.	5.5	More Details
CVE-2024-22103	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	5.5	More Details
CVE-2023-51778	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	5.5	More Details
CVE-2024-25087	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error.	5.5	More Details
CVE-2024-4934	The Quiz and Survey Master (QSM) WordPress plugin before 9.0.2 does not validate and escape some of its Quiz fields before outputting them back in a page/post where the Quiz is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.5	More Details
CVE-2024-22104	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	5.5	More Details
CVE-2024-20896	Use of implicit intent for sensitive communication in Configuration message prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22105	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error.	5.5	More Details
CVE-2024-39322	aimeos/ai-admin-jsonadm is the Aimeos e-commerce JSON API for administrative tasks. In versions prior to 2020.10.13, 2021.10.6, 2022.10.3, 2023.10.4, and 2024.4.2, improper access control allows editors to remove admin group and locale configuration in the Aimeos backend. Versions 2020.10.13, 2021.10.6, 2022.10.3, 2023.10.4, and 2024.4.2 contain a fix for the issue.	5.5	More Details
CVE-2022-25477	Vulnerability in Realtek RtsPer driver for PCIe Card Reader (RtsPer.sys) before 10.0.22000.21355 and Realtek RtsUer driver for USB Card Reader (RtsUer.sys) before 10.0.22000.31274 leaks driver logs that contain addresses of kernel mode objects, weakening KASLR.	5.5	More Details
CVE-2024-4627	The Rank Math SEO WordPress plugin before 1.0.219 does not sanitise and escape some of its settings, which could allow users with access to the General Settings (by default admin, however such access can be given to lower roles via the Role Manager feature of the Rank Math SEO WordPress plugin before 1.0.219) to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	5.4	More Details
CVE-2024-5933	A Cross-site Scripting (XSS) vulnerability exists in the chat functionality of parisneo/lollms-webui in the latest version. This vulnerability allows an attacker to inject malicious scripts via chat messages, which are then executed in the context of the user's browser.	5.4	More Details
CVE-2024-37741	OpenPLC 3 through 9cd8f1b allows XSS via an SVG document as a profile picture.	5.4	More Details
CVE-2024-6375	A command for refining a collection shard key is missing an authorization check. This may cause the command to run directly on a shard, leading to either degradation of query performance, or to revealing chunk boundaries through timing side channels. This affects MongoDB Server v5.0 versions, prior to 5.0.22, MongoDB Server v6.0 versions, prior to 6.0.11 and MongoDB Server v7.0 versions prior to 7.0.3.	5.4	More Details
CVE-2024-28795	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 286832.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3633	The WebP & SVG Support WordPress plugin through 1.4.0 does not sanitise uploaded SVG files, which could allow users with a role as low as Author to upload a malicious SVG containing XSS payloads.	5.4	More Details
CVE-2024-5728	The Animated AL List WordPress plugin through 1.0.6 does not sanitise and escape a parameter 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	5.4	More Details
CVE-2024-28794	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 286831.	5.4	More Details
CVE-2023-50952	IBM InfoSphere Information Server 11.7 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: 275774.	5.4	More Details
CVE-2023-50964	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 276102.	5.4	More Details
CVE-2024-31898	IBM InfoSphere Information Server 11.7 could allow an authenticated user to read or modify sensitive information by bypassing authentication using insecure direct object references. IBM X-Force ID: 288182.	5.4	More Details
CVE-2023-50953	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned. This information could be used in further attacks against the system. IBM X-Force ID: 275775.	5.4	More Details
CVE-2023-42014	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.2.0.2 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 265511.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-36992	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, a low-privileged user that does not hold the admin or power Splunk roles could craft a malicious payload through a View that could result in execution of unauthorized JavaScript code in the browser of a user. The “url” parameter of the Dashboard element does not have proper input validation to reject invalid URLs, which could lead to a Persistent Cross-site Scripting (XSS) exploit.	5.4	More Details
CVE-2024-36993	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, a low-privileged user that does not hold the admin or power Splunk roles could craft a malicious payload through a Splunk Web Bulletin Messages that could result in execution of unauthorized JavaScript code in the browser of a user.	5.4	More Details
CVE-2024-36387	Serving WebSocket protocol upgrades over a HTTP/2 connection could result in a Null Pointer dereference, leading to a crash of the server process, degrading performance.	5.4	More Details
CVE-2024-38527	ZenUML is JavaScript-based diagramming tool that requires no server, using Markdown-inspired text definitions and a renderer to create and modify sequence diagrams. Markdown-based comments in the ZenUML diagram syntax are susceptible to Cross-site Scripting (XSS). The comment feature allows the user to attach small notes for reference. This feature allows the user to enter in their comment in markdown comment, allowing them to use common markdown features, such as `**` for bolded text. However, the markdown text is currently not sanitized before rendering, allowing an attacker to enter a malicious payload for the comment which leads to XSS. This puts existing applications that use ZenUML unsandboxed at risk of arbitrary JavaScript execution when rendering user-controlled diagrams. This vulnerability was patched in version 3.23.25,	5.4	More Details
CVE-2024-36994	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, a low-privileged user that does not hold the admin or power Splunk roles could craft a malicious payload through a View and Splunk Web Bulletin Messages that could result in execution of unauthorized JavaScript code in the browser of a user.	5.4	More Details
CVE-2024-39119	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via admin/info_deal.php?mudi=rev&nohrefStr=close.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5199	The Spotify Play Button WordPress plugin through 1.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2024-39143	A stored cross-site scripting (XSS) vulnerability exists in ResidenceCMS 2.10.1 that allows a low-privilege user to create malicious property content with HTML inside which acts as a stored XSS payload.	5.4	More Details
CVE-2024-6283	The DethemeKit For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the URL parameter of the De Gallery widget in all versions up to and including 2.1.5 due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user clicks on the injected link.	5.4	More Details
CVE-2024-23737	Cross Site Request Forgery (CSRF) vulnerability in savignano S/Notify before 4.0.2 for Jira allows attackers to allows attackers to manipulate a user's S/MIME certificate of PGP key via malicious link or email.	5.4	More Details
CVE-2024-39310	The Basil recipe theme for WordPress is vulnerable to Persistent Cross-Site Scripting (XSS) via the `post_title` parameter in versions up to, and including, 2.0.4 due to insufficient input sanitization and output escaping. This vulnerability allows authenticated attackers with contributor-level access and above to inject arbitrary web scripts in pages that will execute whenever a user accesses a compromised page. Because the of the default WordPress validation, it is not possible to insert the payload directly but if the Cooked plugin is installed, it is possible to create a recipe post type (cp_recipe) and inject the payload in the title field. Version 2.0.5 contains a patch for the issue.	5.4	More Details
CVE-2024-5863	The Easy Image Collage plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the ajax_image_collage() function in all versions up to, and including, 1.13.5. This makes it possible for authenticated attackers, with Contributor-level access and above, to erase all of the content in arbitrary posts.	5.4	More Details
CVE-2024-3111	The Interactive Content WordPress plugin before 1.15.8 does not validate uploads which could allow a Contributors and above to update malicious SVG files, leading to Stored Cross-Site Scripting issues	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25041	IBM Cognos Analytics 11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 12.0.0, 12.0.1, and 12.0.2 is potentially vulnerable to cross site scripting (XSS). A remote attacker could execute malicious commands due to improper validation of column headings in Cognos Assistant. IBM X-Force ID: 282780.	5.4	More Details
CVE-2024-37764	MachForm up to version 19 is affected by an authenticated stored cross-site scripting.	5.4	More Details
CVE-2024-37763	MachForm up to version 19 is affected by an unauthenticated stored cross-site scripting which affects users with valid sessions whom can view compiled forms results.	5.4	More Details
CVE-2024-36995	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, a low-privileged user that does not hold the admin or power Splunk roles could create experimental items.	5.4	More Details
CVE-2024-34592	Improper input validation in parsing RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability.	5.3	More Details
CVE-2024-36996	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.109, an attacker could determine whether or not another user exists on the instance by deciphering the error response that they would likely receive from the instance when they attempt to log in. This disclosure could then lead to additional brute-force password-guessing attacks. This vulnerability would require that the Splunk platform instance uses the Security Assertion Markup Language (SAML) authentication scheme.	5.3	More Details
CVE-2024-34588	Improper input validation흫in parsing RTCP SR packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability.	5.3	More Details
CVE-2024-31883	IBM Security Verify Access 10.0.0.0 through 10.0.7.1, under certain configurations, could allow an unauthenticated attacker to cause a denial of service due to asymmetric resource consumption. IBM X-Force ID: 287615.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34590	Improper input validation흀in parsing an item type from RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability.	5.3	More Details
CVE-2024-20890	Improper input validation in BLE prior to SMR Jul-2024 Release 1 allows adjacent attackers to trigger abnormal behavior.	5.3	More Details
CVE-2023-7270	An issue was discovered in SoftMaker Office 2024 / NX before revision 1214 and SoftMaker FreeOffice 2014 before revision 1215. FreeOffice 2021 is also affected, but won't be fixed. The SoftMaker Office and FreeOffice MSI installer files were found to produce a visible conhost.exe window running as the SYSTEM user when using the repair function of msiexec.exe. This allows a local, low-privileged attacker to use a chain of actions, to open a fully functional cmd.exe with the privileges of the SYSTEM user.	5.3	More Details
CVE-2024-38322	IBM Storage Defender - Resiliency Service 2.0.0 through 2.0.4 agent username and password error response discrepancy exposes product to brute force enumeration. IBM X-Force ID: 294869.	5.3	More Details
CVE-2024-34591	Improper input validation in parsing an item data from RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability.	5.3	More Details
CVE-2024-34589	Improper input validation in parsing RTCP RR packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability.	5.3	More Details
CVE-2024-35119	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in a stack trace. This information could be used in further attacks against the system. IBM X-Force ID: 290342.	5.3	More Details
CVE-2024-38375	@fastly/js-compute is a JavaScript SDK and runtime for building Fastly Compute applications. The implementation of several functions were determined to include a use-after-free bug. This bug could allow for unintended data loss if the result of the preceding functions were sent anywhere else, and often results in a guest trap causing services to return a 500. This bug has been fixed in version 3.16.0 of the `@fastly/js-compute` package.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34580	Apache XML Security for C++ through 2.0.4 implements the XML Signature Syntax and Processing (XMLDsig) specification without protection against an SSRF payload in a KeyInfo element. NOTE: the project disputes this CVE Record on the grounds that any vulnerabilities are the result of a failure to configure XML Security for C++ securely. Even when avoiding this particular issue, any use of this library would need considerable additional code and a deep understanding of the standards and protocols involved to arrive at a secure implementation for any particular use case. We recommend against continued direct use of this library.	5.3	More Details
CVE-2024-39891	In the Twilio Authy API, accessed by Authy Android before 25.1.0 and Authy iOS before 26.1.0, an unauthenticated endpoint provided access to certain phone-number data, as exploited in the wild in June 2024. Specifically, the endpoint accepted a stream of requests containing phone numbers, and responded with information about whether each phone number was registered with Authy. (Authy accounts were not compromised, however.)	5.3	More Details
CVE-2024-39325	aimeos/ai-controller-frontend is the Aimeos frontend controller. Prior to versions 2024.04.2, 2023.10.9, 2022.10.8, 2021.10.8, and 2020.10.15, aimeos/ai-controller-frontend doesn't reset the payment status of a user's basket after the user completes a purchase. Versions 2024.04.2, 2023.10.9, 2022.10.8, 2021.10.8, and 2020.10.15 fix this issue.	5.3	More Details
CVE-2024-38520	SoftEtherVPN is a an open-source cross-platform multi-protocol VPN Program. When SoftEtherVPN is deployed with L2TP enabled on a device, it introduces the possibility of the host being used for amplification/reflection traffic generation because it will respond to every packet with two response packets that are larger than the request packet size. These sorts of techniques are used by external actors who generate spoofed source IPs to target a destination on the internet. This vulnerability has been patched in version 5.02.5185.	5.3	More Details
CVE-2024-2795	The SEO SIMPLE PACK plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 3.2.1 via META description. This makes it possible for unauthenticated attackers to extract limited information about password protected posts.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6414	A vulnerability classified as problematic has been found in Parsec Automation TrakSYS 11.x.x. Affected is an unknown function of the file TS/export/contentpage of the component Export Page. The manipulation of the argument ID leads to direct request. 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-270000. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2023-41927	The server supports at least one cipher suite which is on the NCSC-NL list of cipher suites to be phased out, increasing the risk of cryptographic weaknesses.	5.3	More Details
CVE-2023-47803	A vulnerability regarding improper limitation of a pathname to a restricted directory ('Path Traversal') is found in the Language Settings functionality. This allows remote attackers to read specific files containing non-sensitive information via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	5.3	More Details
CVE-2024-5545	The Motors – Car Dealer, Classifieds & Listing plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the stm_edit_delete_user_car function in all versions up to, and including, 1.4.8. This makes it possible for unauthenticated attackers to unpublish arbitrary posts and pages.	5.3	More Details
CVE-2024-39129	Heap Buffer Overflow vulnerability in DumpTS v0.1.0-nightly allows attackers to cause a denial of service via the function PushTSBuf() at /src/PayloadBuf.cpp.	5.3	More Details
CVE-2024-22276	VMware Cloud Director Object Storage Extension contains an Insertion of Sensitive Information vulnerability. A malicious actor with adjacent access to web/proxy server logging may be able to obtain sensitive information from URLs that are logged.	5.3	More Details
CVE-2024-6099	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to unauthenticated bypass to user registration in versions up to, and including, 4.2.6.8.1. This is due to missing checks in the 'check_validate_fields' function in the checkout. This makes it possible for unauthenticated attackers to register as the default role on the site, even if registration is disabled.	5.3	More Details
CVE-2024-2191	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.9 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows merge request title to be visible publicly despite being set as project members only.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6088	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to unauthorized user registration due to a missing capability check on the 'register' function in all versions up to, and including, 4.2.6.8.1. This makes it possible for unauthenticated attackers to bypass disabled user registration to create a new account with the default role.	5.3	More Details
CVE-2024-5755	In lunary-ai/lunary versions <=v1.2.11, an attacker can bypass email validation by using a dot character ('.') in the email address. This allows the creation of multiple accounts with essentially the same email address (e.g., 'attacker123@gmail.com' and 'attacker.123@gmail.com'), leading to incorrect synchronization and potential security issues.	5.3	More Details
CVE-2023-41928	The device is observed to accept deprecated TLS protocols, increasing the risk of cryptographic weaknesses.	5.3	More Details
CVE-2024-5710	berriai/litellm version 1.34.34 is vulnerable to improper access control in its team management functionality. This vulnerability allows attackers to perform unauthorized actions such as creating, updating, viewing, deleting, blocking, and unblocking any teams, as well as adding or deleting any member to or from any teams. The vulnerability stems from insufficient access control checks in various team management endpoints, enabling attackers to exploit these functionalities without proper authorization.	5.3	More Details
CVE-2024-1816	An issue was discovered in GitLab CE/EE affecting all versions starting from 12.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows for an attacker to cause a denial of service using a crafted OpenAPI file.	5.3	More Details
CVE-2024-4106	A vulnerability has been found in FAST/TOOLS and CI Server. The affected products have built-in accounts with no passwords set. Therefore, if the product is operated without a password set by default, an attacker can break into the affected product. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04 CI Server R1.01.00 to R1.03.00	5.3	More Details
CVE-2024-0158	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability to modify a UEFI variable, leading to denial of service and escalation of privileges	5.1	More Details
CVE-2024-39430	In faceid servive, 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	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39429	In faceid servive, 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	5.1	More Details
CVE-2024-39427	In trusty 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	5.1	More Details
CVE-2024-2819	Incorrect Default Permissions, Improper Preservation of Permissions vulnerability in Hitachi Ops Center Common Services allows File Manipulation.This issue affects Hitachi Ops Center Common Services: before 11.0.2-00.	5.1	More Details
CVE-2024-39879	In JetBrains TeamCity before 2024.03.3 application token could be exposed in EC2 Cloud Profile settings	5.0	More Details
CVE-2024-22231	Syndic cache directory creation is vulnerable to a directory traversal attack in salt project which can lead a malicious attacker to create an arbitrary directory on a Salt master.	5.0	More Details
CVE-2024-5866	Vulnerability in Delinea Centrify PAS v. 21.3 and possibly others. The application is prone to the path traversal vulnerability allowing listing of arbitrary directory outside the root directory of the web application. Versions 23.1-HF7 and on have the patch.	5.0	More Details
CVE-2024-39352	A vulnerability regarding incorrect authorization is found in the firmware upgrade functionality. This allows remote authenticated users with administrator privileges to bypass firmware integrity check via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.7-0298 may be affected: BC500 and TC500.	4.9	More Details
CVE-2024-22272	VMware Cloud Director contains an Improper Privilege Management vulnerability. An authenticated tenant administrator for a given organization within VMware Cloud Director may be able to accidentally disable their organization leading to a Denial of Service for active sessions within their own organization's scope.	4.9	More Details
CVE-2024-3122	CHANGING Mobile One Time Password does not properly filter parameters for the file download functionality, allowing remote attackers with administrator privilege to read arbitrary file on the system.	4.9	More Details
CVE-2024-3999	The EazyDocs WordPress plugin before 2.5.0 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 Number	Description	Base Score	Reference
CVE-2024-35153	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 292640.	4.8	More Details
CVE-2024-6130	The Form Maker by 10Web WordPress plugin before 1.15.26 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-2024-4959	The Frontend Checklist WordPress plugin through 2.3.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-5169	The Video Widget WordPress plugin through 1.2.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-38271	There exists a vulnerability in Quick Share/Nearby, where an attacker can force a victim to stay connected to a temporary hotspot created for the sharing. As part of the sequence of packets in a Quick Share connection over Bluetooth, the attacker forces the victim to connect to the attacker's WiFi network and then sends an OfflineFrame that crashes Quick Share. This makes the Wifi connection to the attacker's network last, instead of returning to the old network when the Quick Share session completes, allowing the attacker to be a MiTM. We recommend upgrading to version 1.0.1724.0 of Quick Share or above	4.8	More Details
CVE-2024-4664	The WP Chat App WordPress plugin before 3.6.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admins to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed.	4.8	More Details
CVE-2024-39314	toy-blog is a headless content management system implementation. Starting in version 0.4.3 and prior to version 0.5.0, the administrative password was leaked through the command line parameter. The problem was patched in version 0.5.0. As a workaround, pass `--read-bearer-token-from-stdin` to the launch arguments and feed the token from the standard input in version 0.4.14 or later. Earlier versions do not have this workaround.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6288	The Conversios – Google Analytics 4 (GA4), Meta Pixel & more Via Google Tag Manager For WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘tiktok_user_id’ parameter in all versions up to, and including, 7.0.12 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	4.7	More Details
CVE-2024-39153	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/info_deal.php?mudi=del&dataType=news&dataTypeCN.	4.7	More Details
CVE-2024-5727	The Widget4Call WordPress plugin through 1.0.7 does not sanitise and escape a parameter 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	4.7	More Details
CVE-2024-38518	BigBlueButton is an open-source virtual classroom designed to help teachers teach and learners learn. An attacker with a valid join link to a meeting can trick BigBlueButton into generating a signed join link with additional parameters. One of those parameters may be "role=moderator", allowing an attacker to join a meeting as moderator using a join link that was originally created for viewer access. This vulnerability has been patched in version(s) 2.6.18, 2.7.8 and 3.0.0-alpha.7.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34696	GeoServer is an open source server that allows users to share and edit geospatial data. Starting in version 2.10.0 and prior to versions 2.24.4 and 2.25.1, GeoServer's Server Status page and REST API lists all environment variables and Java properties to any GeoServer user with administrative rights as part of those modules' status message. These variables/properties can also contain sensitive information, such as database passwords or API keys/tokens. Additionally, many community-developed GeoServer container images `export` other credentials from their start-up scripts as environment variables to the GeoServer (`java`) process. The precise scope of the issue depends on which container image is used and how it is configured. The `about status` API endpoint which powers the Server Status page is only available to administrators.Depending on the operating environment, administrators might have legitimate access to credentials in other ways, but this issue defeats more sophisticated controls (like break-glass access to secrets or role accounts).By default, GeoServer only allows same-origin authenticated API access. This limits the scope for a third-party attacker to use an administrator’s credentials to gain access to credentials. The researchers who found the vulnerability were unable to determine any other conditions under which the GeoServer REST API may be available more broadly. Users should update container images to use GeoServer 2.24.4 or 2.25.1 to get the bug fix. As a workaround, leave environment variables and Java system properties hidden by default. Those who provide the option to re-enable it should communicate the impact and risks so that users can make an informed choice.	4.5	More Details
CVE-2024-34597	Improper input validation in Samsung Health prior to version 6.27.0.113 allows local attackers to write arbitrary document files to the sandbox of Samsung Health. User interaction is required for triggering this vulnerability.	4.4	More Details
CVE-2024-29174	Dell Data Domain, versions prior to 7.13.0.0, LTS 7.7.5.30, LTS 7.10.1.20 contain an SQL Injection vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain SQL commands on the application's backend database causing unauthorized access to application data.	4.4	More Details
CVE-2024-39303	Weblate is a web based localization tool. Prior to version 5.6.2, Weblate didn't correctly validate filenames when restoring project backup. It may be possible to gain unauthorized access to files on the server using a crafted ZIP file. This issue has been addressed in Weblate 5.6.2. As a workaround, do not allow untrusted users to create projects.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39326	SkillTree is a micro-learning gamification platform. Prior to version 2.12.6, the endpoint `/admin/projects/{projectname}/skills/{skillname}/video` (and probably others) is open to a cross-site request forgery (CSRF) vulnerability. Due to the endpoint being CSRFable e.g POST request, supports a content type that can be exploited (multipart file upload), makes a state change and has no CSRF mitigations in place (samesite flag, CSRF token). It is possible to perform a CSRF attack against a logged in admin account, allowing an attacker that can target a logged in admin of Skills Service to modify the videos, captions, and text of the skill. Version 2.12.6 contains a patch for this issue.	4.4	More Details
CVE-2024-34600	Improper verification of intent by broadcast receiver vulnerability in Samsung Flow prior to version 4.9.13.0 allows local attackers to copy image files to external storage.	4.4	More Details
CVE-2024-6011	The Cost Calculator Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘textarea.description’ parameter in all versions up to, and including, 3.2.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details
CVE-2024-32853	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.2 contain an execution with unnecessary privileges vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to escalation of privileges.	4.4	More Details
CVE-2024-37098	Server-Side Request Forgery (SSRF) vulnerability in Blossom Themes BlossomThemes Email Newsletter.This issue affects BlossomThemes Email Newsletter: from n/a through 2.2.6.	4.4	More Details
CVE-2024-27867	An authentication issue was addressed with improved state management. This issue is fixed in AirPods Firmware Update 6A326, AirPods Firmware Update 6F8, and Beats Firmware Update 6F8. When your headphones are seeking a connection request to one of your previously paired devices, an attacker in Bluetooth range might be able to spoof the intended source device and gain access to your headphones.	4.3	More Details
CVE-2024-20894	Improper handling of exceptional conditions in Secure Folder prior to SMR Jul-2024 Release 1 allows physical attackers to bypass authentication under certain condition. User interaction is required for triggering this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4957	The Frontend Checklist WordPress plugin through 2.3.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.3	More Details
CVE-2024-38272	There exists a vulnerability in Quick Share/Nearby, where an attacker can bypass the accept file dialog on Quick Share Windows. Normally in Quick Share Windows app we can't send a file without the user accept from the receiving device if the visibility is set to everyone mode or contacts mode. We recommend upgrading to version 1.0.1724.0 of Quick Share or above	4.3	More Details
CVE-2024-39459	In rare cases Jenkins Plain Credentials Plugin 182.v468b_97b_9dcb_8 and earlier stores secret file credentials unencrypted (only Base64 encoded) on the Jenkins controller file system, where they can be viewed by users with access to the Jenkins controller file system (global credentials) or with Item/Extended Read permission (folder-scoped credentials).	4.3	More Details
CVE-2024-39460	Jenkins Bitbucket Branch Source Plugin 886.v44cf5e4ecec5 and earlier prints the Bitbucket OAuth access token as part of the Bitbucket URL in the build log in some cases.	4.3	More Details
CVE-2024-6012	The Cost Calculator Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'embed-create-page' and 'embed-insert-pages' functions in all versions up to, and including, 3.2.12. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create arbitrary posts and append arbitrary content to existing posts.	4.3	More Details
CVE-2024-29953	A vulnerability in the web interface in Brocade Fabric OS before v9.2.1, v9.2.0b, and v9.1.1d prints encoded session passwords on session storage for Virtual Fabric platforms. This could allow an authenticated user to view other users' session encoded passwords.	4.3	More Details
CVE-2024-5942	The Page and Post Clone plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 6.0 via the 'content_clone' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Author-level access and above, to clone and read private posts.	4.3	More Details
CVE-2024-1330	The kadence-blocks-pro WordPress plugin before 2.3.8 does not prevent users with at least the contributor role using some of its shortcode's functionalities to leak arbitrary options from the database.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6086	In version 1.2.7 of lunary-ai/lunary, any authenticated user, regardless of their role, can change the name of an organization due to improper access control. The function checkAccess() is not implemented, allowing users with the lowest privileges, such as the 'Prompt Editor' role, to modify organization attributes without proper authorization.	4.3	More Details
CVE-2023-42011	IBM Sterling B2B Integrator Standard Edition 6.1 and 6.2 does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with. IBM X-Force ID: 265508.	4.3	More Details
CVE-2023-50954	IBM InfoSphere Information Server 11.7 returns sensitive information in URL information that could be used in further attacks against the system. IBM X-Force ID: 275776.	4.3	More Details
CVE-2024-36987	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200, an authenticated, low-privileged user who does not hold the admin or power Splunk roles could upload a file with an arbitrary extension using the indexing/preview REST endpoint.	4.3	More Details
CVE-2024-31902	IBM InfoSphere Information Server 11.7 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: 289234.	4.3	More Details
CVE-2024-29038	tpm2-tools is the source repository for the Trusted Platform Module (TPM2.0) tools. A malicious attacker can generate arbitrary quote data which is not detected by `tpm2 checkquote`. This issue was patched in version 5.7.	4.3	More Details
CVE-2024-1153	Improper Access Control vulnerability in Talya Informatics Travel APPS allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Travel APPS: before v17.0.68.	4.3	More Details
CVE-2024-3115	An issue was discovered in GitLab EE affecting all versions starting from 16.0 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows an attacker to access issues and epics without having an SSO session using Duo Chat.	4.3	More Details
CVE-2024-37571	Buffer Overflow vulnerability in SAS Broker 9.2 build 1495 allows attackers to cause denial of service or obtain sensitive information via crafted payload to the '_debug' parameter.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6355	A vulnerability was found in Genexis Tilgin Fiber Home Gateway HG1522 CSx000-01_09_01_12. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /status/product_info/. The manipulation of the argument product_info leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-269755. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-5864	The Easy Affiliate Links plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the eafl_reset_settings AJAX action in all versions up to, and including, 3.7.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to reset the plugin's settings.	4.3	More Details
CVE-2024-29040	This repository hosts source code implementing the Trusted Computing Group's (TCG) TPM2 Software Stack (TSS). The JSON Quote Info returned by Fapi_Quote has to be deserialized by Fapi_VerifyQuote to the TPM Structure `TPMS_ATTEST`. For the field `TPM2_GENERATED magic` of this structure any number can be used in the JSON structure. The verifier can receive a state which does not represent the actual, possibly malicious state of the device under test. The malicious device might get access to data it shouldn't, or can use services it shouldn't be able to. This issue has been patched in version 4.1.0.	4.3	More Details
CVE-2024-39133	Heap Buffer Overflow vulnerability in zziplib v0.13.77 allows attackers to cause a denial of service via the __zzip_parse_root_directory() function at /zzip/zip.c.	4.3	More Details
CVE-2024-38857	Improper neutralization of input in Checkmk before versions 2.3.0p8, 2.2.0p28, 2.1.0p45, and 2.0.0 (EOL) allows attackers to craft malicious links that can facilitate phishing attacks.	4.3	More Details
CVE-2024-37138	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 on DDMC contain a relative path traversal vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to the application sending over an unauthorized file to the managed system.	4.1	More Details
CVE-2024-39878	In JetBrains TeamCity before 2024.03.3 private key could be exposed via testing GitHub App Connection	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38480	"Piccoma" App for Android and iOS versions prior to 6.20.0 uses a hard-coded API key for an external service, which may allow a local attacker to obtain the API key. Note that the users of the app are not directly affected by this vulnerability.	4.0	More Details
CVE-2022-38383	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.11.0 and IBM QRadar Software Suite 1.10.12.0 through 1.10.21.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 233673.	4.0	More Details
CVE-2024-34599	Improper input validation in Tips prior to version 6.2.9.4 in Android 14 allows local attacker to send broadcast with Tips' privilege.	4.0	More Details
CVE-2024-6381	The bson_strfreev function in the MongoDB C driver library may be susceptible to an integer overflow where the function will try to free memory at a negative offset. This may result in memory corruption. This issue affected libbson versions prior to 1.26.2	4.0	More Details
CVE-2024-5473	The Simple Photoswipe WordPress plugin through 0.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.0	More Details
CVE-2024-23765	An issue was discovered on HMS Anybus X-Gateway AB7832-F 3 devices. The gateway exposes an unidentified service on port 7412 on the network. All the network services of the gateway become unresponsive after sending 85 requests to this port. The content and length of the frame does not matter. The device needs to be restarted to resume operations.	4.0	More Details
CVE-2024-20900	Improper authentication in MTP application prior to SMR Jul-2024 Release 1 allows local attackers to enter MTP mode without proper authentication.	4.0	More Details
CVE-2024-20899	Use of implicit intent for sensitive communication in RCS function in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information.	4.0	More Details
CVE-2024-20898	Use of implicit intent for sensitive communication in SoftphoneClient in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information.	4.0	More Details
CVE-2024-20897	Use of implicit intent for sensitive communication in FCM function in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34583	Improper access control in system property prior to SMR Jul-2024 Release 1 allows local attackers to get device identifier.	4.0	More Details
CVE-2024-39156	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/keyWord_deal.php?mudi=add.	3.8	More Details
CVE-2024-39157	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/ipRecord_deal.php?mudi=del&dataType=&dataID=1.	3.8	More Details
CVE-2024-37137	Dell Key Trust Platform, v3.0.6 and prior, contains Use of a Cryptographic Primitive with a Risky Implementation vulnerability. A local privileged attacker could potentially exploit this vulnerability, leading to privileged information disclosure.	3.8	More Details
CVE-2024-39324	aimeos/ai-admin-graphql is the Aimeos GraphQL API admin interface. Starting in version 2022.04.1 and prior to versions 2022.10.10, 2023.10.6, and 2024.4.2, improper access control allows a editors to manage own services via GraphQL API which isn't allowed in the JQAdm front end. Versions 2022.10.10, 2023.10.6, and 2024.4.2 contain a patch for the issue.	3.8	More Details
CVE-2024-39302	BigBlueButton is an open-source virtual classroom designed to help teachers teach and learners learn. An attacker may be able to exploit the overly elevated file permissions in the `/usr/local/bigbluebutton/core/vendor/bundle/ruby/2.7.0/gems/resque-2.6.0` directory with the goal of privilege escalation, potentially exposing sensitive information on the server. This issue has been patched in version(s) 2.6.18, 2.7.8 and 3.0.0-alpha.7.	3.7	More Details
CVE-2024-30109	HCL DRYiCE AEX is impacted by a lack of clickjacking protection in the AEX web application. An attacker can use multiple transparent or opaque layers to trick a user into clicking on a button or link on another page than the one intended.	3.7	More Details
CVE-2024-30110	HCL DRYiCE AEX product is impacted by lack of input validation vulnerability in a particular web application. A malicious script can be injected into a system which can cause the system to behave in unexpected ways.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38531	Nix is a package manager for Linux and other Unix systems that makes package management reliable and reproducible. A build process has access to and can change the permissions of the build directory. After creating a setuid binary in a globally accessible location, a malicious local user can assume the permissions of a Nix daemon worker and hijack all future builds. This issue was patched in version(s) 2.23.1, 2.22.2, 2.21.3, 2.20.7, 2.19.5 and 2.18.4.	3.6	More Details
CVE-2024-39846	NewPass before 1.2.0 stores passwords (rather than password hashes) directly, which makes it easier to obtain unauthorized access to sensitive information. NOTE: in each case, data at rest is encrypted, but is decrypted within process memory during use.	3.5	More Details
CVE-2024-24764	October is a self-hosted CMS platform based on the Laravel PHP Framework. This issue affects authenticated administrators who may be redirected to an untrusted URL using the PageFinder schema. The resolver for the page finder link schema (`october://`) allowed external links, therefore allowing an open redirect outside the scope of the active host. This vulnerability has been patched in version 3.5.15.	3.5	More Details
CVE-2024-6369	A vulnerability classified as problematic has been found in LabVantage LIMS 2017. Affected is an unknown function of the file /labvantage/rc?command=page&sdcid=LV_ReagentLot of the component POST Request Handler. The manipulation of the argument mode 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. VDB-269802 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-6367	A vulnerability was found in LabVantage LIMS 2017. It has been declared as problematic. This vulnerability affects unknown code of the file /labvantage/rc?command=file&file=WEB-CORE/elements/files/filesembedded.jsp of the component POST Request Handler. The manipulation of the argument sdcid/keyid1/keyid2/keyid3 leads to cross site scripting. 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-269800. 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-2024-6368	A vulnerability was found in LabVantage LIMS 2017. It has been rated as problematic. This issue affects some unknown processing of the file /labvantage/rc?command=page of the component POST Request Handler. The manipulation of the argument param1 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-269801 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-2024-37141	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain an open redirect vulnerability. A remote low privileged attacker could potentially exploit this vulnerability, leading to information disclosure.	3.5	More Details
CVE-2024-6374	A vulnerability was found in lahirudanushka School Management System 1.0.0/1.0.1 and classified as problematic. This issue affects some unknown processing of the file /subject.php of the component Subject Page. The manipulation of the argument Subject Title/Sybillus Details 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-269807.	3.5	More Details
CVE-2024-6370	A vulnerability classified as problematic was found in LabVantage LIMS 2017. Affected by this vulnerability is an unknown functionality of the file /labvantage/rc?command=file&file=WEB-OPAL/pagetypes/bulletins/sendbulletin.jsp of the component POST Request Handler. The manipulation of the argument bulletinbody leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-269803.	3.5	More Details
CVE-2024-39307	Kavita is a cross platform reading server. Opening an ebook with malicious scripts inside leads to code execution inside the browsing context. Kavita doesn't sanitize or sandbox the contents of epubs, allowing scripts inside ebooks to execute. This vulnerability was patched in version 0.8.1.	3.5	More Details
CVE-2024-30135	HCL DRYiCE AEX is potentially impacted by disclosure of sensitive information in the mobile application when a snapshot is taken.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30111	HCL DRYiCE AEX product is impacted by Missing Root Detection vulnerability in the mobile application. The mobile app can be installed in the rooted device due to which malicious users can gain unauthorized access to the rooted devices, compromising security and potentially leading to data breaches or other malicious activities.	3.3	More Details
CVE-2023-35022	IBM InfoSphere Information Server 11.7 could allow a local user to update projects that they do not have the authorization to access. IBM X-Force ID: 258254.	3.3	More Details
CVE-2024-36278	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause apps crash through type confusion.	3.3	More Details
CVE-2024-31071	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause apps crash through type confusion.	3.3	More Details
CVE-2024-4011	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.1 prior to 16.11.5, starting from 17.0 prior to 17.0.3, and starting from 17.1 prior to 17.1.1, which allows non-project member to promote key results to objectives.	3.1	More Details
CVE-2024-25637	October is a self-hosted CMS platform based on the Laravel PHP Framework. The X-October-Request-Handler Header does not sanitize the AJAX handler name and allows unescaped HTML to be reflected back. There is no impact since this vulnerability cannot be exploited through normal browser interactions. This unescaped value is only detectable when using a proxy interception tool. This issue has been patched in version 3.5.15.	3.1	More Details
CVE-2024-39458	When Jenkins Structs Plugin 337.v1b_04ea_4df7c8 and earlier fails to configure a build step, it logs a warning message containing diagnostic information that may contain secrets passed as step parameters, potentially resulting in accidental exposure of secrets through the default system log.	3.1	More Details
CVE-2024-29177	Dell PowerProtect DD, versions prior to 8.0, LTS 7.13.1.0, LTS 7.10.1.30, LTS 7.7.5.40 contain a disclosure of temporary sensitive information vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to the reuse of disclosed information to gain unauthorized access to the application report.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28830	Insertion of Sensitive Information into Log File in Checkmk GmbH's Checkmk versions <2.3.0p7, <2.2.0p28, <2.1.0p45 and <=2.0.0p39 (EOL) causes automation user secrets to be written to audit log files accessible to administrators.	2.7	More Details
CVE-2024-38364	DSpace is an open source software is a turnkey repository application used by more than 2,000 organizations and institutions worldwide to provide durable access to digital resources. In DSpace 7.0 through 7.6.1, when an HTML, XML or JavaScript Bitstream is downloaded, the user's browser may execute any embedded JavaScript. If that embedded JavaScript is malicious, there is a risk of an XSS attack. This vulnerability has been patched in version 7.6.2.	2.6	More Details
CVE-2024-6344	A vulnerability, which was classified as problematic, was found in ZKTeco ZKBio CVSecurity V5000 4.1.0. This affects an unknown part of the component Push Configuration Section. The manipulation of the argument Configuration Name leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-269733 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2024-6415	A vulnerability classified as problematic was found in Ingenico Estate Manager 2023. Affected by this vulnerability is an unknown functionality of the file /emgui/rest/preferences/PREF_HOME_PAGE/sponsor/3/ of the component New Widget Handler. The manipulation of the argument URL 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-270001 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38537	Fides is an open-source privacy engineering platform. `fides.js`, a client-side script used to interact with the consent management features of Fides, used the `polyfill.io` domain in a very limited edge case, when it detected a legacy browser such as IE11 that did not support the fetch standard. Therefore it was possible for users of legacy, pre-2017 browsers who navigate to a page serving `fides.js` to download and execute malicious scripts from the `polyfill.io` domain when the domain was compromised and serving malware. No exploitation of `fides.js` via `polyfill.io` has been identified as of time of publication. The vulnerability has been patched in Fides version `2.39.1`. Users are advised to upgrade to this version or later to secure their systems against this threat. On Thursday, June 27, 2024, Cloudflare and Namecheap intervened at a domain level to ensure `polyfill.io` and its subdomains could not resolve to the compromised service, rendering this vulnerability unexploitable. Prior to the domain level intervention, there were no server-side workarounds and the confidentiality, integrity, and availability impacts of this vulnerability were high. Clients could ensure they were not affected by using a modern browser that supported the fetch standard.	0.0	More Details
CVE-2024-6085	A path traversal vulnerability exists in the XTTS server included in the lollms package, version v9.6. This vulnerability arises from the ability to perform an unauthenticated root folder settings change. Although the read file endpoint is protected against path traversals, this protection can be bypassed by changing the root folder to '/'. This allows attackers to read arbitrary files on the system. Additionally, the output folders can be changed to write arbitrary audio files to any location on the system.	N/A	More Details
CVE-2022-41729	Rejected reason: reserved but not needed	N/A	More Details
CVE-2022-41730	Rejected reason: reserved but not needed	N/A	More Details
CVE-2023-39324	Rejected reason: reserved but not needed	N/A	More Details
CVE-2024-5334	A local file read vulnerability exists in the stitionai/devika repository, affecting the latest version. The vulnerability is due to improper handling of the 'snapshot_path' parameter in the '/api/get-browser-snapshot' endpoint. An attacker can exploit this vulnerability by crafting a request with a malicious 'snapshot_path' parameter, leading to arbitrary file read from the system. This issue impacts the security of the application by allowing unauthorized access to sensitive files on the server.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5181	A command injection vulnerability exists in the mudler/localai version 2.14.0. The vulnerability arises from the application's handling of the backend parameter in the configuration file, which is used in the name of the initialized process. An attacker can exploit this vulnerability by manipulating the path of the vulnerable binary file specified in the backend parameter, allowing the execution of arbitrary code on the system. This issue is due to improper neutralization of special elements used in an OS command, leading to potential full control over the affected system.	N/A	More Details
CVE-2024-6341	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-34584	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. Reason: An additional patch is required.	N/A	More Details
CVE-2024-5926	A path traversal vulnerability in the get-project-files functionality of stitionai/devika allows attackers to read arbitrary files from the filesystem and cause a Denial of Service (DoS). This issue is present in all versions of the application. The vulnerability arises due to insufficient path sanitization for the 'project-name' parameter, enabling attackers to specify paths that traverse the filesystem. By setting 'project-name' to the root directory, an attacker can cause the application to attempt to read the entire filesystem, leading to a DoS condition.	N/A	More Details
CVE-2024-38515	Rejected reason: This CVE is a duplicate of CVE-2024-38374.	N/A	More Details
CVE-2022-41726	Rejected reason: reserved but not needed	N/A	More Details
CVE-2024-5972	Rejected reason: CVE ID issued in error. This is not a valid vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6354	Improper access control in PAM dashboard in Devolutions Remote Desktop Manager 2024.2.11 and earlier on Windows allows an authenticated user to bypass the execute permission via the use of the PAM dashboard.	N/A	More Details
CVE-2024-3995	In Helix ALM versions prior to 2024.2.0, a local command injection was identified. Reported by Bryan Riggins.	N/A	More Details
CVE-2024-5712	A Cross-Site Request Forgery (CSRF) vulnerability was identified in the stitionai/devika application, affecting the latest version. This vulnerability allows attackers to perform unauthorized actions in the context of a victim's browser, such as deleting projects or changing application settings, without any CSRF protection implemented. Successful exploitation disrupts the integrity and availability of the application and its data.	N/A	More Details
CVE-2024-33328	A cross-site scripting (XSS) vulnerability in the component main.jsp of Lumisxp v15.0.x to v16.1.x allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the pageId parameter.	N/A	More Details
CVE-2024-5827	Vanna v0.3.4 is vulnerable to SQL injection in its DuckDB integration exposed to its Flask Web APIs. Attackers can inject malicious SQL training data and generate corresponding queries to write arbitrary files on the victim's file system, such as backdoor.php with contents `<?php system($_GET[0]); ?>`. This can lead to command execution or the creation of backdoors.	N/A	More Details
CVE-2024-33329	A hardcoded privileged ID within Lumisxp v15.0.x to v16.1.x allows attackers to bypass authentication and access internal pages and other sensitive information.	N/A	More Details
CVE-2022-41728	Rejected reason: reserved but not needed	N/A	More Details
CVE-2022-3428	Rejected reason: reserved but not needed	N/A	More Details
CVE-2022-41718	Rejected reason: reserved but not needed	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32191	Rejected reason: reserved but not needed	N/A	More Details
CVE-2024-6139	A path traversal vulnerability exists in the XTTS server of the parisneo/lollms package version v9.6. This vulnerability allows an attacker to write audio files to arbitrary locations on the system and enumerate file paths. The issue arises from improper validation of user-provided file paths in the `tts_to_file` endpoint.	N/A	More Details
CVE-2024-6250	An absolute path traversal vulnerability exists in parisneo/lollms-webui v9.6, specifically in the `open_file` endpoint of `lollms_advanced.py`. The `sanitize_path` function with `allow_absolute_path=True` allows an attacker to access arbitrary files and directories on a Windows system. This vulnerability can be exploited to read any file and list arbitrary directories on the affected system.	N/A	More Details
CVE-2024-6038	A Regular Expression Denial of Service (ReDoS) vulnerability exists in the latest version of gaizhenbiao/chuanhuchatgpt. The vulnerability is located in the filter_history function within the utils.py module. This function takes a user-provided keyword and attempts to match it against chat history filenames using a regular expression search. Due to the lack of sanitization or validation of the keyword parameter, an attacker can inject a specially crafted regular expression, leading to a denial of service condition. This can cause severe degradation of service performance and potential system unavailability.	N/A	More Details
CVE-2016-20022	In the Linux kernel before 4.8, usb_parse_endpoint in drivers/usb/core/config.c does not validate the wMaxPacketSize field of an endpoint descriptor. NOTE: This vulnerability only affects products that are no longer supported by the supplier.	N/A	More Details
CVE-2024-5980	A vulnerability in the /v1/runs API endpoint of lightning-ai/pytorch-lightning v2.2.4 allows attackers to exploit path traversal when extracting tar.gz files. When the LightningApp is running with the plugin_server, attackers can deploy malicious tar.gz plugins that embed arbitrary files with path traversal vulnerabilities. This can result in arbitrary files being written to any directory in the victim's local file system, potentially leading to remote code execution.	N/A	More Details
CVE-2024-6349	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-2024-5979	In h2oai/h2o-3 version 3.46.0, the `run_tool` command in the `rapids` component allows the `main` function of any class under the `water.tools` namespace to be called. One such class, `MojoConvertTool`, crashes the server when invoked with an invalid argument, causing a denial of service.	N/A	More Details
CVE-2024-5936	An open redirect vulnerability exists in imartinez/privategpt version 0.5.0 due to improper handling of the 'file' parameter. This vulnerability allows attackers to redirect users to a URL specified by user-controlled input without proper validation or sanitization. The impact of this vulnerability includes potential phishing attacks, malware distribution, and credential theft.	N/A	More Details
CVE-2024-4897	parisneo/lollms-webui, in its latest version, is vulnerable to remote code execution due to an insecure dependency on llama-cpp-python version llama_cpp_python-0.2.61+cpuavx2-cp311-cp311-manylinux_2_31_x86_64. The vulnerability arises from the application's 'binding_zoo' feature, which allows attackers to upload and interact with a malicious model file hosted on hugging-face, leading to remote code execution. The issue is linked to a known vulnerability in llama-cpp-python, CVE-2024-34359, which has not been patched in lollms-webui as of commit b454f40a. The vulnerability is exploitable through the application's handling of model files in the 'bindings_zoo' feature, specifically when processing gguf format model files.	N/A	More Details
CVE-2024-5826	In the latest version of vanna-ai/vanna, the `vanna.ask` function is vulnerable to remote code execution due to prompt injection. The root cause is the lack of a sandbox when executing LLM-generated code, allowing an attacker to manipulate the code executed by the `exec` function in `src/vanna/base/base.py`. This vulnerability can be exploited by an attacker to achieve remote code execution on the app backend server, potentially gaining full control of the server.	N/A	More Details
CVE-2024-20081	In gnss service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08719602; Issue ID: MSV-1412.	N/A	More Details
CVE-2024-20079	In gnss service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08044040; Issue ID: MSV-1491.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5824	A path traversal vulnerability in the `/set_personality_config` endpoint of parisneo/lollms version 9.4.0 allows an attacker to overwrite the `configs/config.yaml` file. This can lead to remote code execution by changing server configuration properties such as `force_accept_remote_access` and `turn_on_code_validation`.	N/A	More Details
CVE-2024-36802	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2024-5822	A Server-Side Request Forgery (SSRF) vulnerability exists in the upload processing interface of gaizhenbiao/ChuanhuChatGPT versions <= ChuanhuChatGPT-20240410-git.zip. This vulnerability allows attackers to send crafted requests from the vulnerable server to internal or external resources, potentially bypassing security controls and accessing sensitive data.	N/A	More Details
CVE-2024-5820	An unprotected WebSocket connection in the latest version of stitionai/devika (commit ecee79f) allows a malicious website to connect to the backend and issue commands on behalf of the user. The backend serves all listeners on the given socket, enabling any such malicious website to intercept all communication between the user and the backend. This vulnerability can lead to unauthorized command execution and potential server-side request forgery.	N/A	More Details
CVE-2024-3826	In versions of Akana in versions prior to and including 2022.1.3 validation is broken when using the SAML Single Sign-On (SSO) functionality.	N/A	More Details
CVE-2024-2882	SDG Technologies PnPSCADA allows a remote attacker to attach various entities without requiring system authentication. This breach could potentially lead to unauthorized control, data manipulation, and access to sensitive information within the SCADA system.	N/A	More Details
CVE-2024-5548	A directory traversal vulnerability exists in the stitionai/devika repository, specifically within the /api/download-project endpoint. Attackers can exploit this vulnerability by manipulating the 'project_name' parameter in a GET request to download arbitrary files from the system. This issue affects the latest version of the repository. The vulnerability arises due to insufficient input validation in the 'download_project' function, allowing attackers to traverse the directory structure and access files outside the intended directory. This could lead to unauthorized access to sensitive files on the server.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-5547	A directory traversal vulnerability exists in the /api/download-project-pdf endpoint of the stitionai/devika repository, affecting the latest version. The vulnerability arises due to insufficient sanitization of the 'project_name' parameter in the download_project_pdf function. Attackers can exploit this flaw by manipulating the 'project_name' parameter in a GET request to traverse the directory structure and download arbitrary PDF files from the system. This issue allows attackers to access sensitive information that could be stored in PDF format outside the intended directory.	N/A	More Details
CVE-2022-32147	Rejected reason: reserved but not needed	N/A	More Details
CVE-2024-6090	A path traversal vulnerability exists in gaizhenbiao/chuanhuchatgpt version 20240410, allowing any user to delete other users' chat histories. This vulnerability can also be exploited to delete any files ending in `.json` on the target system, leading to a denial of service as users are unable to authenticate.	N/A	More Details