SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 14 February 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-2024-25100	Deserialization of Untrusted Data vulnerability in WP Swings Coupon Referral Program.This issue affects Coupon Referral Program: from n/a through 1.7.2.	10.0	More Details
CVE-2024-24830	OpenObserve is a observability platform built specifically for logs, metrics, traces, analytics, designed to work at petabyte scale. A vulnerability has been identified in the "/api/{org_id}/users" endpoint. This vulnerability allows any authenticated regular user ('member') to add new users with elevated privileges, including the 'root' role, to an organization. This issue circumvents the intended security controls for role assignments. The vulnerability resides in the user creation process, where the payload does not validate the user roles. A regular user can manipulate the payload to assign root-level privileges. This vulnerability leads to Unauthorized Privilege Escalation and significantly compromises the application's role-based access control system. It allows unauthorized control over application resources and poses a risk to data security. All users, particularly those in administrative roles, are impacted. This issue has been addressed in release version 0.8.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25108	Pixelfed is an open source photo sharing platform. When processing requests authorization was improperly and insufficiently checked, allowing attackers to access far more functionality than users intended, including to the administrative and moderator functionality of the Pixelfed server. This vulnerability affects every version of Pixelfed between v0.10.4 and v0.11.9, inclusive. A proof of concept of this vulnerability exists. This vulnerability affects every local user of a Pixelfed server, and can potentially affect the servers' ability to federate. Some user interaction is required to setup the conditions to be able to exercise the vulnerability, but the attacker could conduct this attack time-delayed manner, where user interaction is not actively required. This vulnerability has been addressed in version 0.11.11. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.9	More Details
CVE-2024-25314	Code-projects Hotel Managment System 1.0, allows SQL Injection via the 'sid' parameter in Hotel/admin/show.php?sid=2.	9.8	More Details
CVE-2024-25302	Sourcecodester Event Student Attendance System 1.0, allows SQL Injection via the 'student' parameter.	9.8	More Details
CVE-2023-6677	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Oduyo Financial Technology Online Collection allows SQL Injection.This issue affects Online Collection: before v.1.0.2.	9.8	More Details
CVE-2024-25678	In LiteSpeed QUIC (LSQUIC) Library before 4.0.4, DCID validation is mishandled.	9.8	More Details
CVE-2024-25675	An issue was discovered in MISP before 2.4.184. A client does not need to use POST to start an export generation process. This is related to app/Controller/JobsController.php and app/View/Events/export.ctp.	9.8	More Details
CVE-2024-25674	An issue was discovered in MISP before 2.4.184. Organisation logo upload is insecure because of a lack of checks for the file extension and MIME type.	9.8	More Details
CVE-2024-21762	A out-of-bounds write in Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to execute unauthorized code or commands via specifically crafted requests	9.8	More Details
CVE-2024-24308	SQL Injection vulnerability in Boostmyshop (boostmyshopagent) module for Prestashop versions 1.1.9 and before, allows remote attackers to escalate privileges and obtain sensitive information via changeOrderCarrier.php, relayPoint.php, and shippingConfirmation.php.	9.8	More Details
CVE-2023-50026	SQL injection vulnerability in Presta Monster "Multi Accessories Pro" (hsmultiaccessoriespro) module for PrestaShop versions 5.1.1 and before, allows remote attackers to escalate privileges and obtain sensitive information via the method HsAccessoriesGroupProductAbstract::getAccessoriesByIdProducts().	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46350	SQL injection vulnerability in InnovaDeluxe "Manufacturer or supplier alphabetical search" (idxrmanufacturer) module for PrestaShop versions 2.0.4 and before, allows remote attackers to escalate privileges and obtain sensitive information via the methods IdxrmanufacturerFunctions::getCornersLink, IdxrmanufacturerFunctions::getManufacturersLike and IdxrmanufacturerFunctions::getSuppliersLike.	9.8	More Details
CVE-2023-46687	In Emerson Rosemount GC370XA, GC700XA, and GC1500XA products, an unauthenticated user with network access could execute arbitrary commands in root context from a remote computer.	9.8	More Details
CVE-2024-1284	Use after free in Mojo in Google Chrome prior to 121.0.6167.160 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	9.8	More Details
CVE-2023-47132	An issue discovered in N-able N-central before 2023.6 and earlier allows attackers to gain escalated privileges via API calls.	9.8	More Details
CVE-2024-24393	File Upload vulnerability index.php in Pichome v.1.1.01 allows a remote attacker to execute arbitrary code via crafted POST request.	9.8	More Details
CVE-2023-40266	An issue was discovered in Atos Unify OpenScape Xpressions WebAssistant V7 before V7R1 FR5 HF42 P911. It allows path traversal.	9.8	More Details
CVE-2024-24496	An issue in Daily Habit Tracker v.1.0 allows a remote attacker to manipulate trackers via the home.php, add-tracker.php, delete-tracker.php, update-tracker.php components.	9.8	More Details
CVE-2024-25307	Code-projects Cinema Seat Reservation System 1.0 allows SQL Injection via the 'id' parameter at "/Cinema-Reservation/booking.php?id=1."	9.8	More Details
CVE-2024-25316	Code-projects Hotel Managment System 1.0 allows SQL Injection via the 'eid' parameter in Hotel/admin/usersettingdel.php?eid=2.	9.8	More Details
CVE-2024-25315	Code-projects Hotel Managment System 1.0, allows SQL Injection via the 'rid' parameter in Hotel/admin/roombook.php?rid=2.	9.8	More Details
CVE-2024-22836	An OS command injection vulnerability exists in Akaunting v3.1.3 and earlier. An attacker can manipulate the company locale when installing an app to execute system commands on the hosting server.	9.8	More Details
CVE-2024-21413	Microsoft Outlook Remote Code Execution Vulnerability	9.8	More Details
CVE-2024-21410	Microsoft Exchange Server Elevation of Privilege Vulnerability	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21401	Microsoft Entra Jira Single-Sign-On Plugin Elevation of Privilege Vulnerability	9.8	More Details
CVE-2024-22923	SQL injection vulnerability in adv radius v.2.2.5 allows a local attacker to execute arbitrary code via a crafted script.	9.8	More Details
CVE-2024-23816	A vulnerability has been identified in Location Intelligence Perpetual Large (9DE5110-8CA13-1AX0) (All versions < V4.3), Location Intelligence Perpetual Medium (9DE5110-8CA12-1AX0) (All versions < V4.3), Location Intelligence Perpetual Non-Prod (9DE5110-8CA10-1AX0) (All versions < V4.3), Location Intelligence Perpetual Small (9DE5110-8CA11-1AX0) (All versions < V4.3), Location Intelligence SUS Large (9DE5110-8CA13-1BX0) (All versions < V4.3), Location Intelligence SUS Medium (9DE5110-8CA12-1BX0) (All versions < V4.3), Location Intelligence SUS Non-Prod (9DE5110-8CA10-1BX0) (All versions < V4.3), Location Intelligence SUS Small (9DE5110-8CA11-1BX0) (All versions < V4.3). Affected products use a hard-coded secret value for the computation of a Keyed-Hash Message Authentication Code. This could allow an unauthenticated remote attacker to gain full administrative access to the application.	9.8	More Details
CVE-2023-42374	An issue in mystenlabs Sui Blockchain before v.1.6.3 allow a remote attacker to execute arbitrary code and cause a denial of service via a crafted compressed script to the Sui node component.	9.8	More Details
CVE-2024-23763	SQL Injection vulnerability in Gambio through 4.9.2.0 allows attackers to run arbitrary SQL commands via crafted GET request using modifiers[attribute][] parameter.	9.8	More Details
CVE-2024-23761	Server Side Template Injection in Gambio 4.9.2.0 allows attackers to run arbitrary code via crafted smarty email template.	9.8	More Details
CVE-2024-23759	Deserialization of Untrusted Data in Gambio through 4.9.2.0 allows attackers to run arbitrary code via "search" parameter of the Parcelshopfinder/AddAddressBookEntry" function.	9.8	More Details
CVE-2024-25110	The UAMQP is a general purpose C library for AMQP 1.0. During a call to open_get_offered_capabilities, a memory allocation may fail causing a use-after-free issue and if a client called it during connection communication it may cause a remote code execution. Users are advised to update the submodule with commit `30865c9c`. There are no known workarounds for this vulnerability.	9.8	More Details
CVE-2023-6036	The Web3 WordPress plugin before 3.0.0 is vulnerable to an authentication bypass due to incorrect authentication checking in the login flow in functions 'handle_auth_request' and 'hadle_login_request'. This makes it possible for non authenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the username.	9.8	More Details
CVE-2024-24797	Deserialization of Untrusted Data vulnerability in G5Theme ERE Recently Viewed – Essential Real Estate Add-On.This issue affects ERE Recently Viewed – Essential Real Estate Add-On: from n/a through 1.3.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25722	qanything_kernel/connector/database/mysql/mysql_client.py in qanything.ai QAnything before 1.2.0 allows SQL Injection.	9.8	More Details
CVE-2024-25718	In the Samly package before 1.4.0 for Elixir, Samly.State.Store.get_assertion/3 can return an expired session, which interferes with access control because Samly.AuthHandler uses a cached session and does not replace it, even after expiry.	9.8	More Details
CVE-2024-25714	In Rhonabwy through 1.1.13, HMAC signature verification uses a strcmp function that is vulnerable to side-channel attacks, because it stops the comparison when the first difference is spotted in the two signatures. (The fix uses gnutls_memcmp, which has constant-time execution.)	9.8	More Details
CVE-2024-24495	SQL Injection vulnerability in delete-tracker.php in Daily Habit Tracker v.1.0 allows a remote attacker to execute arbitrary code via crafted GET request.	9.8	More Details
CVE-2024-1283	Heap buffer overflow in Skia in Google Chrome prior to 121.0.6167.160 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	9.8	More Details
CVE-2024-24321	An issue in Dlink DIR-816A2 v.1.10CNB05 allows a remote attacker to execute arbitrary code via the wizardstep4_ssid_2 parameter in the sub_42DA54 function.	9.8	More Details
CVE-2024-24025	An arbitrary File upload vulnerability exists in Novel-Plus v4.3.0-RC1 and prior at com.java2nb.common.controller.FileController: upload(). An attacker can pass in specially crafted filename parameter to perform arbitrary File download.	9.8	More Details
CVE-2024-24023	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior. An attacker can pass specially crafted offset, limit, and sort parameters to perform SQL injection via /novel/bookContent/list.	9.8	More Details
CVE-2024-24018	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior versions. An attacker can pass in crafted offset, limit, and sort parameters to perform SQL injection via /system/dataPerm/list	9.8	More Details
CVE-2023-38995	An issue in SCHUHFRIED v.8.22.00 allows remote attacker to obtain the database password via crafted curl command.	9.8	More Details
CVE-2024-24213	Supabase PostgreSQL v15.1 was discovered to contain a SQL injection vulnerability via the component /pg_meta/default/query. NOTE: the vendor's position is that this is an intended feature; also, it exists in the Supabase dashboard product, not the Supabase PostgreSQL product. Specifically, /pg_meta/default/query is for SQL queries that are entered in an intended UI by an authorized user. Nothing is injected.	9.8	More Details
CVE-2024-24811	SQLAlchemyDA is a generic database adapter for ZSQL methods. A vulnerability found in versions prior to 2.2 allows unauthenticated execution of arbitrary SQL statements on the database to which the SQLAlchemyDA instance is connected. All users are affected. The problem has been patched in version 2.2. There is no workaround for the problem.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24189	Jsish v3.5.0 (commit 42c694c) was discovered to contain a use-after-free via the SplitChar at ./src/jsiUtils.c.	9.8	More Details
CVE-2024-24188	Jsish v3.5.0 was discovered to contain a heap-buffer-overflow in ./src/jsiUtils.c.	9.8	More Details
CVE-2024-24186	Jsish v3.5.0 (commit 42c694c) was discovered to contain a stack-overflow via the component IterGetKeysCallback at /jsish/src/jsiValue.c.	9.8	More Details
CVE-2024-24133	Atmail v6.6.0 was discovered to contain a SQL injection vulnerability via the username parameter on the login page.	9.8	More Details
CVE-2024-24303	SQL Injection vulnerability in HiPresta "Gift Wrapping Pro" (hiadvancedgiftwrapping) module for PrestaShop before version 1.4.1, allows remote attackers to escalate privileges and obtain sensitive information via the HiAdvancedGiftWrappingGiftWrappingModuleFrontController::addGiftWrappingCartValue() method.	9.8	More Details
CVE-2023-46914	SQL Injection vulnerability in RM bookingcalendar module for PrestaShop versions 2.7.9 and before, allows remote attackers to execute arbitrary code, escalate privileges, and obtain sensitive information via ics_export.php.	9.8	More Details
CVE-2024-24019	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior versions. An attacker can pass in crafted offset, limit, and sort parameters to perform SQL injection via /system/roleDataPerm/list	9.8	More Details
CVE-2024-24004	jshERP v3.3 is vulnerable to SQL Injection. The com.jsh.erp.controller.DepotHeadController: com.jsh.erp.utils.BaseResponseInfo findInOutDetail() function of jshERP does not filter `column` and `order` parameters well enough, and an attacker can construct malicious payload to bypass jshERP's protection mechanism in `safeSqlParse` method for sql injection.	9.8	More Details
CVE-2024-24002	jshERP v3.3 is vulnerable to SQL Injection. The com.jsh.erp.controller.MaterialController: com.jsh.erp.utils.BaseResponseInfo getListWithStock() function of jshERP does not filter `column` and `order` parameters well enough, and an attacker can construct malicious payload to bypass jshERP's protection mechanism in `safeSqlParse` method for sql injection.	9.8	More Details
CVE-2024-24001	jshERP v3.3 is vulnerable to SQL Injection. via the com.jsh.erp.controller.DepotHeadController: com.jsh.erp.utils.BaseResponseInfo findallocationDetail() function of jshERP which allows an attacker to construct malicious payload to bypass jshERP's protection mechanism.	9.8	More Details
CVE-2024-24024	An arbitrary File download vulnerability exists in Novel-Plus v4.3.0-RC1 and prior at com.java2nb.common.controller.FileController: fileDownload(). An attacker can pass in specially crafted filePath and fieName parameters to perform arbitrary File download.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24563	Vyper is a Pythonic Smart Contract Language for the Ethereum Virtual Machine. Arrays can be keyed by a signed integer, while they are defined for unsigned integers only. The typechecker doesn't throw when spotting the usage of an `int` as an index for an array. The typechecker allows the usage of signed integers to be used as indexes to arrays. The vulnerability is present in different forms in all versions, including `0.3.10`. For ints, the 2's complement representation is used. Because the array was declared very large, the bounds checking will pass Negative values will simply be represented as very large numbers. As of time of publication, a fixed version does not exist. There are three potential vulnerability classes: unpredictable behavior, accessing inaccessible elements and denial of service. Class 1: If it is possible to index an array with a negative integer without reverting, this is most likely not anticipated by the developer and such accesses can cause unpredictable behavior for the contract. Class 2: If a contract has an invariant in the form `assert index < x`, the developer will suppose that no elements on indexes `y | y >= x` are accessible. However, by using negative indexes, this can be bypassed. Class 3: If the index is dependent on the state of the contract, this poses a risk of denial of service. If the state of the contract can be manipulated in such way that the index will be forced to be negative, the array access can always revert (because most likely the array won't be declared extremely large). However, all these the scenarios are highly unlikely. Most likely behavior is a revert on the bounds check.	9.8	More Details
CVE-2024-24026	An arbitrary File upload vulnerability exists in Novel-Plus v4.3.0-RC1 and prior versions at com.java2nb.system.controller.SysUserController: uploadImg(). An attacker can pass in specially crafted filename parameter to perform arbitrary File download.	9.8	More Details
CVE-2024-24202	An arbitrary file upload vulnerability in /upgrade/control.php of ZenTao Community Edition v18.10, ZenTao Biz v8.10, and ZenTao Max v4.10 allows attackers to execute arbitrary code via uploading a crafted .txt file.	9.8	More Details
CVE-2023-50061	PrestaShop Op'art Easy Redirect >= 1.3.8 and <= 1.3.12 is vulnerable to SQL Injection via Oparteasyredirect::hookActionDispatcher().	9.8	More Details
CVE-2024-25191	php-jwt 1.0.0 uses strcmp (which is not constant time) to verify authentication, which makes it easier to bypass authentication via a timing side channel.	9.8	More Details
CVE-2024-25190	l8w8jwt 2.2.1 uses memcmp (which is not constant time) to verify authentication, which makes it easier to bypass authentication via a timing side channel.	9.8	More Details
CVE-2024-25189	libjwt 1.15.3 uses strcmp (which is not constant time) to verify authentication, which makes it easier to bypass authentication via a timing side channel.	9.8	More Details
CVE-2023-42282	The ip package before 1.1.9 for Node.js might allow SSRF because some IP addresses (such as 0x7f.1) are improperly categorized as globally routable via isPublic.	9.8	More Details
CVE-2024-22394	An improper authentication vulnerability has been identified in SonicWall SonicOS SSL-VPN feature, which in specific conditions could allow a remote attacker to bypass authentication. This issue affects only firmware version SonicOS 7.1.1-7040.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1207	The WP Booking Calendar plugin for WordPress is vulnerable to SQL Injection via the 'calendar_request_params[dates_ddmmyy_csv]' parameter in all versions up to, and including, 9.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.8	More Details
CVE-2024-24216	Zentao v18.0 to v18.10 was discovered to contain a remote code execution (RCE) vulnerability via the checkConnection method of /app/zentao/module/repo/model.php.	9.8	More Details
CVE-2024-24091	Yealink Meeting Server before v26.0.0.66 was discovered to contain an OS command injection vulnerability via the file upload interface.	9.8	More Details
CVE-2024-24142	Sourcecodester School Task Manager 1.0 allows SQL Injection via the 'subject' parameter.	9.8	More Details
CVE-2024-24021	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior. An attacker can pass specially crafted offset, limit, and sort parameters to perform SQL injection via /novel/userFeedback/list.	9.8	More Details
CVE-2024-24017	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior versions. An attacker can pass crafted offset, limit, and sort parameters to perform SQL injection via /common/dict/list	9.8	More Details
CVE-2024-24014	A SQL injection vulnerability exists in Novel-Plus v4.3.0-RC1 and prior versions. An attacker can pass crafted offset, limit, and sort parameters to perform SQL injection via /novel/author/list	9.8	More Details
CVE-2024-24003	jshERP v3.3 is vulnerable to SQL Injection. The com.jsh.erp.controller.DepotHeadController: com.jsh.erp.utils.BaseResponseInfo findInOutMaterialCount() function of jshERP does not filter `column` and `order` parameters well enough, and an attacker can construct malicious payload to bypass jshERP's protection mechanism in `safeSqlParse` method for sql injection.	9.8	More Details
CVE-2024-25145	Stored cross-site scripting (XSS) vulnerability in the Portal Search module's Search Result app in Liferay Portal 7.2.0 through 7.4.3.11, and older unsupported versions, and Liferay DXP 7.4 before update 8, 7.3 before update 4, 7.2 before fix pack 17, and older unsupported versions allows remote authenticated users to inject arbitrary web script or HTML into the Search Result app's search result if highlighting is disabled by adding any searchable content (e.g., blog, message board message, web content article) to the application.	9.6	More Details
CVE-2024-20254	Multiple vulnerabilities in Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an unauthenticated, remote attacker to conduct cross-site request forgery (CSRF) attacks that perform arbitrary actions on an affected device. Note: "Cisco Expressway Series" refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. For more information about these vulnerabilities, see the Details ["#details"] section of this advisory.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48974	Cross Site Scripting vulnerability in Axigen WebMail prior to 10.3.3.61 allows a remote attacker to escalate privileges via a crafted script to the serverName_input parameter.	9.6	More Details
CVE-2024-20252	Multiple vulnerabilities in Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an unauthenticated, remote attacker to conduct cross-site request forgery (CSRF) attacks that perform arbitrary actions on an affected device. Note: "Cisco Expressway Series" refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. For more information about these vulnerabilities, see the Details ["#details"] section of this advisory.	9.6	More Details
CVE-2024-21364	Microsoft Azure Site Recovery Elevation of Privilege Vulnerability	9.3	More Details
CVE-2024-1355	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance via the actions-console docker container while setting a service URL. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program.	9.1	More Details
CVE-2024-1378	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance via nomad templates when configuring SMTP options. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program https://bounty.github.com .	9.1	More Details
CVE-2024-1374	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance via nomad templates when configuring audit log forwarding. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program https://bounty.github.com .	9.1	More Details
CVE-2024-1372	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance when configuring SAML settings. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program https://bounty.github.com .	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1369	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance when setting the username and password for collectd configurations. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program https://bounty.github.com .	9.1	More Details
CVE-2024-1359	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance when setting up an HTTP proxy. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program https://bounty.github.com .	9.1	More Details
CVE-2024-22131	In SAP ABA (Application Basis) - versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75I, an attacker authenticated as a user with a remote execution authorization can use a vulnerable interface. This allows the attacker to use the interface to invoke an application function to perform actions which they would not normally be permitted to perform. Depending on the function executed, the attack can read or modify any user/business data and can make the entire system unavailable.	9.1	More Details
CVE-2022-48623	The Cpanel::JSON::XS package before 4.33 for Perl performs out-of-bounds accesses in a way that allows attackers to obtain sensitive information or cause a denial of service.	9.1	More Details
CVE-2024-25106	OpenObserve is a observability platform built specifically for logs, metrics, traces, analytics, designed to work at petabyte scale. A critical vulnerability has been identified in the "/api/{org_id}/users/{email_id}" endpoint. This vulnerability allows any authenticated user within an organization to remove any other user from that same organization, irrespective of their respective roles. This includes the ability to remove users with "Admin" and "Root" roles. By enabling any organizational member to unilaterally alter the user base, it opens the door to unauthorized access and can cause considerable disruptions in operations. The core of the vulnerability lies in the `remove_user_from_org` function in the user management system. This function is designed to allow organizational users to remove members from their organization. The function does not check if the user initiating the request has the appropriate administrative privileges to remove a user. Any user who is part of the organization, irrespective of their role, can remove any other user, including those with higher privileges. This vulnerability is categorized as an Authorization issue leading to Unauthorized User Removal. The impact is severe, as it compromises the integrity of user management within organizations. By exploiting this vulnerability, any user within an organization, without the need for administrative privileges, can remove critical users, including "Admins" and "Root" users. This could result in unauthorized system access, administrative lockout, or operational disruptions. Given that user accounts are typically created by "Admins" or "Root" users, this vulnerability can be exploited by any user who has been granted access to an organization, thereby posing a critical risk to the security and operational stability of the application. This issue has been addressed in release version 0.8.0. Users are advised to upgrade.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24825	DIRAC is a distributed resource framework. In affected versions any user could get a token that has been requested by another user/agent. This may expose resources to unintended parties. This issue has been addressed in release version 8.0.37. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.1	More Details
CVE-2024-21403	Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability	9.0	More Details
CVE-2024-21376	Microsoft Azure Kubernetes Service Confidential Container Remote Code Execution Vulnerability	9.0	More Details
CVE-2024-23724	Ghost through 5.76.0 allows stored XSS, and resultant privilege escalation in which a contributor can take over any account, via an SVG profile picture that contains JavaScript code to interact with the API on localhost TCP port 3001. NOTE: The discoverer reports that "The vendor does not view this as a valid vector."	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-25448	An issue in the imlib_free_image_and_decache function of imlib2 v1.9.1 allows attackers to cause a heap buffer overflow via parsing a crafted image.	8.8	More Details
CVE-2024-24824	Graylog is a free and open log management platform. Starting in version 2.0.0 and prior to versions 5.1.11 and 5.2.4, arbitrary classes can be loaded and instantiated using a HTTP PUT request to the `/api/system/cluster_config/` endpoint. Graylog's cluster config system uses fully qualified class names as config keys. To validate the existence of the requested class before using them, Graylog loads the class using the class loader. If a user with the appropriate permissions performs the request, arbitrary classes with 1-arg String constructors can be instantiated. This will execute arbitrary code that is run during class instantiation. In the specific use case of `java.io.File`, the behavior of the internal web-server stack will lead to information exposure by including the entire file content in the response to the REST request. Versions 5.1.11 and 5.2.4 contain a fix for this issue.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24821	Composer is a dependency Manager for the PHP language. In affected versions several files within the local working directory are included during the invocation of Composer and in the context of the executing user. As such, under certain conditions arbitrary code execution may lead to local privilege escalation, provide lateral user movement or malicious code execution when Composer is invoked within a directory with tampered files. All Composer CLI commands are affected, including composer.phar's self-update. The following scenarios are of high risk: Composer being run with sudo, Pipelines which may execute Composer on untrusted projects, Shared environments with developers who run Composer individually on the same project. This vulnerability has been addressed in versions 2.7.0 and 2.2.23. It is advised that the patched versions are applied at the earliest convenience. Where not possible, the following should be addressed: Remove all sudo composer privileges for all users to mitigate root privilege escalation, and avoid running Composer within an untrusted directory, or if needed, verify that the contents of `vendor/composer/InstalledVersions.php` and `vendor/composer/installed.php` do not include untrusted code. A reset can also be done on these files by the following:```sh rm vendor/composer/installed.php vendor/composer/InstalledVersions.php composer install --no-scripts --no-plugins ```	8.8	More Details
CVE-2024-21365	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-40263	An issue was discovered in Atos Unify OpenScape Voice Trace Manager V8 before V8 R0.9.11. It allows authenticated command injection via ftp.	8.8	More Details
CVE-2024-25417	flusity-CMS v2.33 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /core/tools/add_translation.php.	8.8	More Details
CVE-2024-21366	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-25418	flusity-CMS v2.33 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /core/tools/delete_menu.php.	8.8	More Details
CVE-2023-40265	An issue was discovered in Atos Unify OpenScape Xpressions WebAssistant V7 before V7R1 FR5 HF42 P911. It allows authenticated remote code execution via file upload.	8.8	More Details
CVE-2023-27001	An issue discovered in Egerie Risk Manager v4.0.5 allows attackers to bypass the signature mechanism and tamper with the values inside the JWT payload resulting in privilege escalation.	8.8	More Details
CVE-2024-21367	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21368	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21369	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-25419	flusity-CMS v2.33 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /core/tools/update_menu.php.	8.8	More Details
CVE-2024-21370	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-25744	In the Linux kernel before 6.6.7, an untrusted VMM can trigger int80 syscall handling at any given point. This is related to arch/x86/coco/tdx/tdx.c and arch/x86/mm/mem_encrypt_amd.c.	8.8	More Details
CVE-2023-47020	Multiple Cross-Site Request Forgery (CSRF) chaining in NCR Terminal Handler v.1.5.1 allows privileges to be escalated by an attacker through a crafted request involving user account creation and adding the user to an administrator group. This is exploited by an undisclosed function in the WSDL that lacks security controls and can accept custom content types.	8.8	More Details
CVE-2024-21372	Windows OLE Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-6515	Authorization Bypass Through User-Controlled Key vulnerability in Mia Technology Inc. MİA-MED allows Authentication Abuse.This issue affects MİA-MED: before 1.0.7.	8.8	More Details
CVE-2024-21375	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-23811	A vulnerability has been identified in SINEC NMS (All versions < V2.0 SP1). The affected application allows users to upload arbitrary files via TFTP. This could allow an attacker to upload malicious firmware images or other files, that could potentially lead to remote code execution.	8.8	More Details
CVE-2024-21378	Microsoft Outlook Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-23810	A vulnerability has been identified in SINEC NMS (All versions < V2.0 SP1). The affected application is vulnerable to SQL injection. This could allow an unauthenticated remote attacker to execute arbitrary SQL queries on the server database.	8.8	More Details
CVE-2024-21361	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21360	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21359	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-25312	Code-projects Simple School Managment System 1.0 allows SQL Injection via the 'id' parameter at "School/sub_delete.php?id=5."	8.8	More Details
CVE-2023-50386	Improper Control of Dynamically-Managed Code Resources, Unrestricted Upload of File with Dangerous Type, Inclusion of Functionality from Untrusted Control Sphere vulnerability in Apache Solr.This issue affects Apache Solr: from 6.0.0 through 8.11.2, from 9.0.0 before 9.4.1. In the affected versions, Solr ConfigSets accepted Java jar and class files to be uploaded through the ConfigSets API. When backing up Solr Collections, these configSet files would be saved to disk when using the LocalFileSystemRepository (the default for backups). If the backup was saved to a directory that Solr uses in its ClassPath/ClassLoaders, then the jar and class files would be available to use with any ConfigSet, trusted or untrusted. When Solr is run in a secure way (Authorization enabled), as is strongly suggested, this vulnerability is limited to extending the Backup permissions with the ability to add libraries. Users are recommended to upgrade to version 8.11.3 or 9.4.1, which fix the issue. In these versions, the following protections have been added: * Users are no longer able to upload files to a configSet that could be executed via a Java ClassLoader. * The Backup API restricts saving backups to directories that are used in the ClassLoader.	8.8	More Details
CVE-2024-21345	Windows Kernel Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-25450	imlib2 v1.9.1 was discovered to mishandle memory allocation in the function init_imlib_fonts().	8.8	More Details
CVE-2024-25447	An issue in the imlib_load_image_with_error_return function of imlib2 v1.9.1 allows attackers to cause a heap buffer overflow via parsing a crafted image.	8.8	More Details
CVE-2024-21349	Microsoft ActiveX Data Objects Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21350	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-25318	Code-projects Hotel Managment System 1.0 allows SQL Injection via the 'pid' parameter in Hotel/admin/print.php?pid=2.	8.8	More Details
CVE-2024-25310	Code-projects Simple School Managment System 1.0 allows SQL Injection via the 'id' parameter at "School/delete.php?id=5."	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25313	Code-projects Simple School Managment System 1.0 allows Authentication Bypass via the username and password parameters at School/teacher_login.php.	8.8	More Details
CVE-2024-25309	Code-projects Simple School Managment System 1.0 allows SQL Injection via the 'pass' parameter at School/teacher_login.php.	8.8	More Details
CVE-2024-0594	The Awesome Support – WordPress HelpDesk & Support Plugin plugin for WordPress is vulnerable to union-based SQL Injection via the 'q' parameter of the wpas_get_users action in all versions up to, and including, 6.1.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2024-25308	Code-projects Simple School Managment System 1.0 allows SQL Injection via the 'name' parameter at School/teacher_login.php.	8.8	More Details
CVE-2024-25306	Code-projects Simple School Managment System 1.0 allows SQL Injection via the 'aname' parameter at "School/index.php".	8.8	More Details
CVE-2024-25305	Code-projects Simple School Managment System 1.0 allows Authentication Bypass via the username and password parameters at School/index.php.	8.8	More Details
CVE-2024-25304	Code-projects Simple School Managment System 1.0 allows SQL Injection via the 'apass' parameter at "School/index.php."	8.8	More Details
CVE-2023-6724	Authorization Bypass Through User-Controlled Key vulnerability in Software Engineering Consultancy Machine Equipment Limited Company Hearing Tracking System allows Authentication Abuse.This issue affects Hearing Tracking System: before for IOS 7.0, for Android Latest release 1.0.	8.8	More Details
CVE-2024-25677	In Min before 1.31.0, local files are not correctly treated as unique security origins, which allows them to improperly request cross-origin resources. For example, a local file may request other local files through an XML document.	8.8	More Details
CVE-2024-21352	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21353	Microsoft WDAC ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21358	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24350	File Upload vulnerability in Software Publico e-Sic Livre v.2.0 and before allows a remote attacker to execute arbitrary code via the extension filtering component.	8.8	More Details
CVE-2024-24113	xxl-job =< 2.4.1 has a Server-Side Request Forgery (SSRF) vulnerability, which causes low-privileged users to control executor to RCE.	8.8	More Details
CVE-2024-21420	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-22454	Dell PowerProtect Data Manager, version 19.15 and prior versions, contain a weak password recovery mechanism for forgotten passwords. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to unauthorized access to the application with privileges of the compromised account. The attacker could retrieve the reset password token without authorization and then perform the password change	8.8	More Details
CVE-2024-21391	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-52431	The Plack::Middleware::XSRFBlock package before 0.0.19 for Perl allows attackers to bypass a CSRF protection mechanism via an empty form value and an empty cookie (if signed cookies are disabled).	8.8	More Details
CVE-2024-22126	The User Admin application of SAP NetWeaver AS for Java - version 7.50, insufficiently validates and improperly encodes the incoming URL parameters before including them into the redirect URL. This results in Cross-Site Scripting (XSS) vulnerability, leading to a high impact on confidentiality and mild impact on integrity and availability.	8.8	More Details
CVE-2024-22022	Vulnerability CVE-2024-22022 allows a Veeam Recovery Orchestrator user that has been assigned a low-privileged role to access the NTLM hash of the service account used by the Veeam Orchestrator Server Service.	8.8	More Details
CVE-2024-1118	The Podlove Subscribe button plugin for WordPress is vulnerable to UNION-based SQL Injection via the 'button' attribute of the podlove-subscribe-button shortcode in all versions up to, and including, 1.3.10 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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-2024-23512	Deserialization of Untrusted Data vulnerability in wpxpo ProductX – WooCommerce Builder & Gutenberg WooCommerce Blocks.This issue affects ProductX – WooCommerce Builder & Gutenberg WooCommerce Blocks: from n/a through 3.1.4.	8.7	More Details
CVE-2024-23513	Deserialization of Untrusted Data vulnerability in PropertyHive.This issue affects PropertyHive: from n/a through 2.0.5.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23324	Envoy is a high-performance edge/middle/service proxy. External authentication can be bypassed by downstream connections. Downstream clients can force invalid gRPC requests to be sent to ext_authz, circumventing ext_authz checks when failure_mode_allow is set to true. This issue has been addressed in released 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.6	More Details
CVE-2024-24743	SAP NetWeaver AS Java (CAF - Guided Procedures) - version 7.50, allows an unauthenticated attacker to submit a malicious request with a crafted XML file over the network, which when parsed will enable him to access sensitive files and data but not modify them. There are expansion limits in place so that availability is not affected.	8.6	More Details
CVE-2024-22024	An XML external entity or XXE vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x) and ZTA gateways which allows an attacker to access certain restricted resources without authentication.	8.3	More Details
CVE-2024-24820	Icinga Director is a tool designed to make Icinga 2 configuration handling easy. Not any of Icinga Director's configuration forms used to manipulate the monitoring environment are protected against cross site request forgery (CSRF). It enables attackers to perform changes in the monitoring environment managed by Icinga Director without the awareness of the victim. Users of the map module in version 1.x, should immediately upgrade to v2.0. The mentioned XSS vulnerabilities in Icinga Web are already fixed as well and upgrades to the most recent release of the 2.9, 2.10 or 2.11 branch must be performed if not done yet. Any later major release is also suitable. Icinga Director will receive minor updates to the 1.8, 1.9, 1.10 and 1.11 branches to remedy this issue. Upgrade immediately to a patched release. If that is not feasible, disable the director module for the time being.	8.3	More Details
CVE-2023-51761	In Emerson Rosemount GC370XA, GC700XA, and GC1500XA products, an unauthenticated user with network access could bypass authentication and acquire admin capabilities.	8.3	More Details
CVE-2024-24796	Deserialization of Untrusted Data vulnerability in MagePeople Team Event Manager and Tickets Selling Plugin for WooCommerce – WpEvently – WordPress Plugin.This issue affects Event Manager and Tickets Selling Plugin for WooCommerce – WpEvently – WordPress Plugin: from n/a through 4.1.1.	8.2	More Details
CVE-2023-43017	IBM Security Verify Access 10.0.0.0 through 10.0.6.1 could allow a privileged user to install a configuration file that could allow remote access. IBM X-Force ID: 266155.	8.2	More Details
CVE-2024-20255	A vulnerability in the SOAP API of Cisco Expressway Series and Cisco TelePresence Video Communication Server could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected system. An attacker could exploit this vulnerability by persuading a user of the REST API to follow a crafted link. A successful exploit could allow the attacker to cause the affected system to reload.	8.2	More Details
CVE-2024-21395	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24810	WiX toolset lets developers create installers for Windows Installer, the Windows installation engine. The .be TEMP folder is vulnerable to DLL redirection attacks that allow the attacker to escalate privileges. This impacts any installer built with the WiX installer framework. This issue has been patched in version 4.0.4.	8.2	More Details
CVE-2024-21357	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	8.1	More Details
CVE-2024-21412	Internet Shortcut Files Security Feature Bypass Vulnerability	8.1	More Details
CVE-2024-23812	A vulnerability has been identified in SINEC NMS (All versions < V2.0 SP1). The affected application incorrectly neutralizes special elements when creating a report which could lead to command injection.	8.0	More Details
CVE-2023-50957	IBM Storage Defender - Resiliency Service 2.0 could allow a privileged user to perform unauthorized actions after obtaining encrypted data from clear text key storage. IBM X-Force ID: 275783.	8.0	More Details
CVE-2024-0985	Late privilege drop in REFRESH MATERIALIZED VIEW CONCURRENTLY in PostgreSQL allows an object creator to execute arbitrary SQL functions as the command issuer. The command intends to run SQL functions as the owner of the materialized view, enabling safe refresh of untrusted materialized views. The victim is a superuser or member of one of the attacker's roles. The attack requires luring the victim into running REFRESH MATERIALIZED VIEW CONCURRENTLY on the attacker's materialized view. Versions before PostgreSQL 16.2, 15.6, 14.11, 13.14, and 12.18 are affected.	8.0	More Details
CVE-2024-21380	Microsoft Dynamics Business Central/NAV Information Disclosure Vulnerability	8.0	More Details
CVE-2024-24337	CSV Injection vulnerability in '/members/moremember.pl' and '/admin/aqbudgets.pl' endpoints in Koha Library Management System version 23.05.05 and earlier allows attackers to to inject DDE commands into csv exports via the 'Budget' and 'Patrons Member' components.	8.0	More Details
CVE-2024-1354	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance via the `syslog-ng` configuration file. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program.	8.0	More Details
CVE-2024-23762	Unrestricted File Upload vulnerability in Content Manager feature in Gambio 4.9.2.0 allows attackers to execute arbitrary code via upload of crafted PHP file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25442	An issue in the HuginBase::PanoramaMemento::loadPTScript function of Hugin v2022.0.0 allows attackers to cause a heap buffer overflow via parsing a crafted image.	7.8	More Details
CVE-2024-22228	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_cifssupport utility. An authenticated attacker could potentially exploit this vulnerability, escaping the restricted shell and execute arbitrary operating system commands with root privileges.	7.8	More Details
CVE-2024-21346	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-25446	An issue in the HuginBase::PTools::setDestImage function of Hugin v2022.0.0 allows attackers to cause a heap buffer overflow via parsing a crafted image.	7.8	More Details
CVE-2023-25365	Cross Site Scripting vulnerability found in October CMS v.3.2.0 allows local attacker to execute arbitrary code via the file type .mp3	7.8	More Details
CVE-2024-23796	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-25445	Improper handling of values in HuginBase::PTools::Transform::transform of Hugin 2022.0.0 leads to an assertion failure.	7.8	More Details
CVE-2024-23795	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-22223	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability within its svc_cbr utility. An authenticated malicious user with local access could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application.	7.8	More Details
CVE-2024-25443	An issue in the HuginBase::ImageVariable<double>::linkWith function of Hugin v2022.0.0 allows attackers to cause a heap-use-after-free via parsing a crafted image.	7.8	More Details
CVE-2024-21363	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-50236	A vulnerability has been identified in Polarion ALM (All versions < V2404.0). The affected product is vulnerable due to weak file and folder permissions in the installation path. An attacker with local access could exploit this vulnerability to escalate privileges to NT AUTHORITY\SYSTEM.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22042	A vulnerability has been identified in Unicam FX (All versions). The windows installer agent used in affected product contains incorrect use of privileged APIs that trigger the Windows Console Host (conhost.exe) as a child process with SYSTEM privileges. This could be exploited by an attacker to perform a local privilege escalation attack.	7.8	More Details
CVE-2024-22227	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_dc utility. An authenticated attacker could potentially exploit this vulnerability, leading to the ability execute commands with root privileges.	7.8	More Details
CVE-2024-20673	Microsoft Office Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-49125	A vulnerability has been identified in Parasolid V35.0 (All versions < V35.0.263), Parasolid V35.1 (All versions < V35.1.252), Parasolid V36.0 (All versions < V36.0.198), Solid Edge SE2023 (All versions < V223.0 Update 11), Solid Edge SE2024 (All versions < V224.0 Update 3). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted files containing XT format. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-21315	Microsoft Defender for Endpoint Protection Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-46757	Insufficient checking of memory buffer in ASP Secure OS may allow an attacker with a malicious TA to read/write to the ASP Secure OS kernel virtual address space potentially leading to privilege escalation.	7.8	More Details
CVE-2024-21354	Microsoft Message Queuing (MSMQ) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-0229	An out-of-bounds memory access flaw was found in the X.Org server. This issue can be triggered when a device frozen by a sync grab is reattached to a different master device. This issue may lead to an application crash, local privilege escalation (if the server runs with extended privileges), or remote code execution in SSH X11 forwarding environments.	7.8	More Details
CVE-2024-25003	KiTTY versions 0.76.1.13 and before is vulnerable to a stack-based buffer overflow via the hostname, occurs due to insufficient bounds checking and input sanitization. This allows an attacker to overwrite adjacent memory, which leads to arbitrary code execution.	7.8	More Details
CVE-2024-25004	KiTTY versions 0.76.1.13 and before is vulnerable to a stack-based buffer overflow via the username, occurs due to insufficient bounds checking and input sanitization (at line 2600). This allows an attacker to overwrite adjacent memory, which leads to arbitrary code execution.	7.8	More Details
CVE-2024-23749	KiTTY versions 0.76.1.13 and before is vulnerable to command injection via the filename variable, occurs due to insufficient input sanitization and validation, failure to escape special characters, and insecure system calls (at lines 2369-2390). This allows an attacker to add inputs inside the filename variable, leading to arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22012	there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-22224	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_nas utility. An authenticated attacker could potentially exploit this vulnerability, escaping the restricted shell and execute arbitrary operating system commands with root privileges.	7.8	More Details
CVE-2024-24922	A vulnerability has been identified in Simcenter Femap (All versions < V2401.0000). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted Catia MODEL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21715)	7.8	More Details
CVE-2024-1149	Improper Verification of Cryptographic Signature vulnerability in Snow Software Inventory Agent on MacOS, Snow Software Inventory Agent on Windows, Snow Software Inventory Agent on Linux allows File Manipulation through Snow Update Packages.This issue affects Inventory Agent: through 6.12.0; Inventory Agent: through 6.14.5; Inventory Agent: through 6.7.2.	7.8	More Details
CVE-2024-24924	A vulnerability has been identified in Simcenter Femap (All versions < V2306.0000). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted Catia MODEL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-22059)	7.8	More Details
CVE-2024-24923	A vulnerability has been identified in Simcenter Femap (All versions < V2401.0000), Simcenter Femap (All versions < V2306.0001). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted Catia MODEL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-22055)	7.8	More Details
CVE-2024-24921	A vulnerability has been identified in Simcenter Femap (All versions < V2401.0000). The affected application is vulnerable to memory corruption while parsing specially crafted Catia MODEL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21712)	7.8	More Details
CVE-2024-24920	A vulnerability has been identified in Simcenter Femap (All versions < V2401.0000). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted Catia MODEL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21710)	7.8	More Details
CVE-2024-23797	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected applications contain a stack overflow vulnerability while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-22225	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_supportassist utility. An authenticated attacker could potentially exploit this vulnerability, leading to execution of arbitrary operating system commands with root privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21379	Microsoft Word Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-23804	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected applications contain a stack overflow vulnerability while parsing specially crafted PSOBJ files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-23803	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions), Tecnomatix Plant Simulation V2302 (All versions < V2302.0007). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-23802	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-0164	Dell Unity, versions prior to 5.4, contain an OS Command Injection Vulnerability in its svc_topstats utility. An authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary commands with elevated privileges.	7.8	More Details
CVE-2024-0165	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_acldb_dump utility. An authenticated attacker could potentially exploit this vulnerability, leading to execution of arbitrary operating system commands with root privileges.	7.8	More Details
CVE-2024-0166	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_tcpdump utility. An authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands with elevated privileges.	7.8	More Details
CVE-2024-0167	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in the svc_topstats utility. An authenticated attacker could potentially exploit this vulnerability, leading to the ability to overwrite arbitrary files on the file system with root privileges.	7.8	More Details
CVE-2024-0168	Dell Unity, versions prior to 5.4, contains a Command Injection Vulnerability in svc_oscheck utility. An authenticated attacker could potentially exploit this vulnerability, leading to the ability to inject arbitrary operating system commands. This vulnerability allows an authenticated attacker to execute commands with root privileges.	7.8	More Details
CVE-2024-0170	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_cava utility. An authenticated attacker could potentially exploit this vulnerability, escaping the restricted shell and execute arbitrary operating system commands with root privileges.	7.8	More Details
CVE-2024-21384	Microsoft Office OneNote Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23798	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected applications contain a stack overflow vulnerability while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-22222	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability within its svc_udoctor utility. An authenticated malicious user with local access could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application.	7.8	More Details
CVE-2024-24925	A vulnerability has been identified in Simcenter Femap (All versions < V2306.0000). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted Catia MODEL files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-22060)	7.8	More Details
CVE-2024-21338	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-1150	Improper Verification of Cryptographic Signature vulnerability in Snow Software Inventory Agent on Unix allows File Manipulation through Snow Update Packages.This issue affects Inventory Agent: through 7.3.1.	7.8	More Details
CVE-2024-24771	Open Forms allows users create and publish smart forms. Versions prior to 2.2.9, 2.3.7, 2.4.5, and 2.5.2 contain a non-exploitable multi-factor authentication weakness. Superusers who have their credentials (username + password) compromised could potentially have the second-factor authentication bypassed if an attacker somehow managed to authenticate to Open Forms. The maintainers of Open Forms do not believe it is or has been possible to perform this login. However, if this were possible, the victim's account may be abused to view (potentially sensitive) submission data or have been used to impersonate other staff accounts to view and/or modify data. Three mitigating factors to help prevent exploitation include: the usual login page (at `/admin/login/`) does not fully log in the user until the second factor was succesfully provided; the additional non-MFA protected login page at `/api/v2/api-authlogin/` was misconfigured and could not be used to log in; and there are no additional ways to log in. This also requires credentials of a superuser to be compromised to be exploitable. Versions 2.2.9, 2.3.7, 2.4.5, and 2.5.2 contain the following patches to address these weaknesses: Move and only enable the API auth endpoints (`/api/v2/api-auth/login/`) with `settings.DEBUG = True`. `settings.DEBUG = True` is insecure and should never be applied in production settings. Additionally, apply a custom permission check to the hijack flow to only allow second-factor-verified superusers to perform user hijacking.	7.7	More Details
CVE-2024-1329	HashiCorp Nomad and Nomad Enterprise 1.5.13 up to 1.6.6, and 1.7.3 template renderer is vulnerable to arbitrary file write on the host as the Nomad client user through symlink attacks. This vulnerability, CVE-2024-1329, is fixed in Nomad 1.7.4, 1.6.7, and 1.5.14.	7.7	More Details
CVE-2024-21327	Microsoft Dynamics 365 Customer Engagement Cross-Site Scripting Vulnerability	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21351	Windows SmartScreen Security Feature Bypass Vulnerability	7.6	More Details
CVE-2024-21394	Dynamics 365 Field Service Spoofing Vulnerability	7.6	More Details
CVE-2024-22130	Print preview option in SAP CRM WebClient UI - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, S4FND 108, WEBCUIF 700, WEBCUIF 701, WEBCUIF 730, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting vulnerability. An attacker with low privileges can cause limited impact to confidentiality and integrity of the appliaction data after successful exploitation.	7.6	More Details
CVE-2024-21393	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	7.6	More Details
CVE-2024-21328	Dynamics 365 Sales Spoofing Vulnerability	7.6	More Details
CVE-2024-21396	Dynamics 365 Sales Spoofing Vulnerability	7.6	More Details
CVE-2024-21389	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	7.6	More Details
CVE-2024-21348	Internet Connection Sharing (ICS) Denial of Service Vulnerability	7.5	More Details
CVE-2023-32328	IBM Security Verify Access 10.0.0.0 through 10.0.6.1 uses insecure protocols in some instances that could allow an attacker on the network to take control of the server. IBM X-Force Id: 254957.	7.5	More Details
CVE-2024-24814	mod_auth_openidc is an OpenID Certified™ authentication and authorization module for the Apache 2.x HTTP server that implements the OpenID Connect Relying Party functionality. In affected versions missing input validation on mod_auth_openidc_session_chunks cookie value makes the server vulnerable to a denial of service (DoS) attack. An internal security audit has been conducted and the reviewers found that if they manipulated the value of the mod_auth_openidc_session_chunks cookie to a very large integer, like 99999999, the server struggles with the request for a long time and finally gets back with a 500 error. Making a few requests of this kind caused our server to become unresponsive. Attackers can craft requests that would make the server work very hard (and possibly become unresponsive) and/or crash with minimal effort. This issue has been addressed in version 2.4.15.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25407	SteVe v3.6.0 was discovered to use predictable transaction ID's when receiving a StartTransaction request. This vulnerability can allow attackers to cause a Denial of Service (DoS) by using the predicted transaction ID's to terminate other transactions.	7.5	More Details
CVE-2024-24781	An unauthenticated remote attacker can use an uncontrolled resource consumption vulnerability to DoS the affected devices through excessive traffic on a single ethernet port.	7.5	More Details
CVE-2024-23322	Envoy is a high-performance edge/middle/service proxy. Envoy will crash when certain timeouts happen within the same interval. The crash occurs when the following are true: 1. hedge_on_per_try_timeout is enabled, 2. per_try_idle_timeout is enabled (it can only be done in configuration), 3. per-try-timeout is enabled, either through headers or configuration and its value is equal, or within the backoff interval of the per_try_idle_timeout. This issue has been addressed in released 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2024-24926	Deserialization of Untrusted Data vulnerability in UnitedThemes Brooklyn	Creative Multi-Purpose Responsive WordPress Theme.This issue affects Brooklyn	Creative Multi-Purpose Responsive WordPress Theme: from n/a through 4.9.7.6.	7.5	More Details
CVE-2024-25200	Espruino 2v20 (commit fcc9ba4) was discovered to contain a Stack Overflow via the jspeFactorFunctionCall at src/jsparse.c.	7.5	More Details
CVE-2024-25201	Espruino 2v20 (commit fcc9ba4) was discovered to contain an Out-of-bounds Read via jsvStringIteratorPrintfCallback at src/jsvar.c.	7.5	More Details
CVE-2024-23756	The HTTP PUT and DELETE methods are enabled in the Plone official Docker version 5.2.13 (5221), allowing unauthenticated attackers to execute dangerous actions such as uploading files to the server or deleting them.	7.5	More Details
CVE-2024-21347	Microsoft ODBC Driver Remote Code Execution Vulnerability	7.5	More Details
CVE-2023-50298	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Solr.This issue affects Apache Solr: from 6.0.0 through 8.11.2, from 9.0.0 before 9.4.1. Solr Streaming Expressions allows users to extract data from other Solr Clouds, using a "zkHost" parameter. When original SolrCloud is setup to use ZooKeeper credentials and ACLs, they will be sent to whatever "zkHost" the user provides. An attacker could setup a server to mock ZooKeeper, that accepts ZooKeeper requests with credentials and ACLs and extracts the sensitive information, then send a streaming expression using the mock server's address in "zkHost". Streaming Expressions are exposed via the "/streaming" handler, with "read" permissions. Users are recommended to upgrade to version 8.11.3 or 9.4.1, which fix the issue. From these versions on, only zkHost values that have the same server address (regardless of chroot), will use the given ZooKeeper credentials and ACLs when connecting.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50292	Incorrect Permission Assignment for Critical Resource, Improper Control of Dynamically-Managed Code Resources vulnerability in Apache Solr. This issue affects Apache Solr: from 8.10.0 through 8.11.2, from 9.0.0 before 9.3.0. The Schema Designer was introduced to allow users to more easily configure and test new Schemas and configSets. However, when the feature was created, the "trust" (authentication) of these configSets was not considered. External library loading is only available to configSets that are "trusted" (created by authenticated users), thus non-authenticated users are unable to perform Remote Code Execution. Since the Schema Designer loaded configSets without taking their "trust" into account, configSets that were created by unauthenticated users were allowed to load external libraries when used in the Schema Designer. Users are recommended to upgrade to version 9.3.0, which fixes the issue.	7.5	More Details
CVE-2023-50291	Insufficiently Protected Credentials vulnerability in Apache Solr. This issue affects Apache Solr: from 6.0.0 through 8.11.2, from 9.0.0 before 9.3.0. One of the two endpoints that publishes the Solr process' Java system properties, /admin/info/properties, was only setup to hide system properties that had "password" contained in the name. There are a number of sensitive system properties, such as "basicauth" and "aws.secretKey" do not contain "password", thus their values were published via the "/admin/info/properties" endpoint. This endpoint populates the list of System Properties on the home screen of the Solr Admin page, making the exposed credentials visible in the UI. This /admin/info/properties endpoint is protected under the "config-read" permission. Therefore, Solr Clouds with Authorization enabled will only be vulnerable through logged-in users that have the "config-read" permission. Users are recommended to upgrade to version 9.3.0 or 8.11.3, which fixes the issue. A single option now controls hiding Java system property for all endpoints, "-Dsolr.hiddenSysProps". By default all known sensitive properties are hidden (including "-Dbasicauth"), as well as any property with a name containing "secret" or "password". Users who cannot upgrade can also use the following Java system property to fix the issue: '-Dsolr.redaction.system.pattern=.*(password|secret|basicauth).*'	7.5	More Details
CVE-2023-5679	A bad interaction between DNS64 and serve-stale may cause `named` to crash with an assertion failure during recursive resolution, when both of these features are enabled. This issue affects BIND 9 versions 9.16.12 through 9.16.45, 9.18.0 through 9.18.21, 9.19.0 through 9.19.19, 9.16.12-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.	7.5	More Details
CVE-2024-25728	ExpressVPN before 12.73.0 on Windows, when split tunneling is used, sends DNS requests according to the Windows configuration (e.g., sends them to DNS servers operated by the user's ISP instead of to the ExpressVPN DNS servers), which may allow remote attackers to obtain sensitive information about websites visited by VPN users.	7.5	More Details
CVE-2024-21386	.NET Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6516	To keep its cache database efficient, `named` running as a recursive resolver occasionally attempts to clean up the database. It uses several methods, including some that are asynchronous: a small chunk of memory pointing to the cache element that can be cleaned up is first allocated and then queued for later processing. It was discovered that if the resolver is continuously processing query patterns triggering this type of cache-database maintenance, `named` may not be able to handle the cleanup events in a timely manner. This in turn enables the list of queued cleanup events to grow infinitely large over time, allowing the configured `max-cache-size` limit to be significantly exceeded. This issue affects BIND 9 versions 9.16.0 through 9.16.45 and 9.16.8-S1 through 9.16.45-S1.	7.5	More Details
CVE-2024-23833	OpenRefine is a free, open source power tool for working with messy data and improving it. A jdbc attack vulnerability exists in OpenRefine(version<=3.7.7) where an attacker may construct a JDBC query which may read files on the host filesystem. Due to the newer MySQL driver library in the latest version of OpenRefine (8.0.30), there is no associated deserialization utilization point, so original code execution cannot be achieved, but attackers can use this vulnerability to read sensitive files on the target server. This issue has been addressed in version 3.7.8. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2024-20290	A vulnerability in the OLE2 file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to an incorrect check for end-of-string values during scanning, which may result in a heap buffer over-read. An attacker could exploit this vulnerability by submitting a crafted file containing OLE2 content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software and consuming available system resources. For a description of this vulnerability, see the ClamAV blog .	7.5	More Details
CVE-2024-24311	Path Traversal vulnerability in Linea Grafica "Multilingual and Multistore Sitemap Pro - SEO" (lgsitemaps) module for PrestaShop before version 1.6.6, a guest can download personal information without restriction.	7.5	More Details
CVE-2023-45191	IBM Engineering Lifecycle Optimization 7.0.2 and 7.0.3 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 268755.	7.5	More Details
CVE-2023-5517	A flaw in query-handling code can cause `named` to exit prematurely with an assertion failure when: - `nxdomain-redirect <domain>;` is configured, and - the resolver receives a PTR query for an RFC 1918 address that would normally result in an authoritative NXDOMAIN response. This issue affects BIND 9 versions 9.12.0 through 9.16.45, 9.18.0 through 9.18.21, 9.19.0 through 9.19.19, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.	7.5	More Details
CVE-2024-24304	In the module "Mailjet" (mailjet) from Mailjet for PrestaShop before versions 3.5.1, a guest can download technical information without restriction.	7.5	More Details
CVE-2024-21404	.NET Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51440	A vulnerability has been identified in SIMATIC CP 343-1 (6GK7343-1EX30-0XE0) (All versions), SIMATIC CP 343-1 Lean (6GK7343-1CX10-0XE0) (All versions), SIPLUS NET CP 343-1 (6AG1343-1EX30-7XE0) (All versions), SIPLUS NET CP 343-1 Lean (6AG1343-1CX10-2XE0) (All versions). Affected products incorrectly validate TCP sequence numbers. This could allow an unauthenticated remote attacker to create a denial of service condition by injecting spoofed TCP RST packets.	7.5	More Details
CVE-2023-4408	The DNS message parsing code in `named` includes a section whose computational complexity is overly high. It does not cause problems for typical DNS traffic, but crafted queries and responses may cause excessive CPU load on the affected `named` instance by exploiting this flaw. This issue affects both authoritative servers and recursive resolvers. This issue affects BIND 9 versions 9.0.0 through 9.16.45, 9.18.0 through 9.18.21, 9.19.0 through 9.19.19, 9.9.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.	7.5	More Details
CVE-2024-21490	This affects versions of the package angular from 1.3.0. A regular expression used to split the value of the ng-srcset directive is vulnerable to super-linear runtime due to backtracking. With large carefully-crafted input, this can result in catastrophic backtracking and cause a denial of service. **Note:** This package is EOL and will not receive any updates to address this issue. Users should migrate to [@angular/core] (https://www.npmjs.com/package/@angular/core).	7.5	More Details
CVE-2024-20667	Azure DevOps Server Remote Code Execution Vulnerability	7.5	More Details
CVE-2023-52427	In OpenDDS through 3.27, there is a segmentation fault for a DataWriter with a large value of resource_limits.max_samples. NOTE: the vendor's position is that the product is not designed to handle a max_samples value that is too large for the amount of memory on the system.	7.5	More Details
CVE-2024-0842	The Backuply – Backup, Restore, Migrate and Clone plugin for WordPress is vulnerable to Denial of Service in all versions up to, and including, 1.2.5. This is due to direct access of the backuply/restore_ins.php file and. This makes it possible for unauthenticated attackers to make excessive requests that result in the server running out of resources.	7.5	More Details
CVE-2024-23327	Envoy is a high-performance edge/middle/service proxy. When PPv2 is enabled both on a listener and subsequent cluster, the Envoy instance will segfault when attempting to craft the upstream PPv2 header. This occurs when the downstream request has a command type of LOCAL and does not have the protocol block. This issue has been addressed in releases 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2023-6519	Exposure of Data Element to Wrong Session vulnerability in Mia Technology Inc. MİA-MED allows Read Sensitive Strings Within an Executable.This issue affects MİA-MED: before 1.0.7.	7.5	More Details
CVE-2023-6518	Plaintext Storage of a Password vulnerability in Mia Technology Inc. MİA-MED allows Read Sensitive Strings Within an Executable.This issue affects MİA-MED: before 1.0.7.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6517	Exposure of Sensitive Information Due to Incompatible Policies vulnerability in Mia Technology Inc. MİA-MED allows Collect Data as Provided by Users.This issue affects MİA-MED: before 1.0.7.	7.5	More Details
CVE-2024-21406	Windows Printing Service Spoofing Vulnerability	7.5	More Details
CVE-2023-32330	IBM Security Verify Access 10.0.0.0 through 10.0.6.1 uses insecure calls that could allow an attacker on the network to take control of the server. IBM X-Force ID: 254977.	7.5	More Details
CVE-2024-21342	Windows DNS Client Denial of Service Vulnerability	7.5	More Details
CVE-2024-23325	Envoy is a high-performance edge/middle/service proxy. Envoy crashes in Proxy protocol when using an address type that isn't supported by the OS. Envoy is susceptible to crashing on a host with IPv6 disabled and a listener config with proxy protocol enabled when it receives a request where the client presents its IPv6 address. It is valid for a client to present its IPv6 address to a target server even though the whole chain is connected via IPv4. This issue has been addressed in released 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2023-52428	In Connect2id Nimbus JOSE+JWT before 9.37.2, an attacker can cause a denial of service (resource consumption) via a large JWE p2c header value (aka iteration count) for the PasswordBasedDecrypter (PBKDF2) component.	7.5	More Details
CVE-2024-23452	Request smuggling vulnerability in HTTP server in Apache bRPC 0.9.5~1.7.0 on all platforms allows attacker to smuggle request. Vulnerability Cause Description： The http_parser does not comply with the RFC-7230 HTTP 1.1 specification. Attack scenario: If a message is received with both a Transfer-Encoding and a Content-Length header field, such a message might indicate an attempt to perform request smuggling or response splitting. One particular attack scenario is that a bRPC made http server on the backend receiving requests in one persistent connection from frontend server that uses TE to parse request with the logic that 'chunk' is contained in the TE field. in that case an attacker can smuggle a request into the connection to the backend server. Solution: You can choose one solution from below: 1. Upgrade bRPC to version 1.8.0, which fixes this issue. Download link: https://github.com/apache/brpc/releases/tag/1.8.0 2. Apply this patch: https://github.com/apache/brpc/pull/2518	7.5	More Details
CVE-2023-47131	The N-able PassPortal extension before 3.29.2 for Chrome inserts sensitive information into a log file.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23660	The Binance Trust Wallet app for iOS in commit 3cd6e8f647fbba8b5d8844fcd144365a086b629f, git tag 0.0.4 misuses the trezor-crypto library and consequently generates mnemonic words for which the device time is the only entropy source, leading to economic losses, as exploited in the wild in July 2023. An attacker can systematically generate mnemonics for each timestamp within an applicable timeframe, and link them to specific wallet addresses in order to steal funds from those wallets.	7.5	More Details
CVE-2024-22132	SAP IDES ECC-systems contain code that permits the execution of arbitrary program code of user's choice.An attacker can therefore control the behaviour of the system by executing malicious code which can potentially escalate privileges with low impact on confidentiality, integrity and availability of the system.	7.4	More Details
CVE-2024-25642	Due to improper validation of certificate in SAP Cloud Connector - version 2.0, attacker can impersonate the genuine servers to interact with SCC breaking the mutual authentication. Hence, the attacker can intercept the request to view/modify sensitive information. There is no impact on the availability of the system.	7.4	More Details
CVE-2023-51437	Observable timing discrepancy vulnerability in Apache Pulsar SASL Authentication Provider can allow an attacker to forge a SASL Role Token that will pass signature verification. Users are recommended to upgrade to version 2.11.3, 3.0.2, or 3.1.1 which fixes the issue. Users should also consider updating the configured secret in the `saslJaasServerRoleTokenSignerSecretPath` file. Any component matching an above version running the SASL Authentication Provider is affected. That includes the Pulsar Broker, Proxy, Websocket Proxy, or Function Worker. 2.11 Pulsar users should upgrade to at least 2.11.3. 3.0 Pulsar users should upgrade to at least 3.0.2. 3.1 Pulsar users should upgrade to at least 3.1.1. Any users running Pulsar 2.8, 2.9, 2.10, and earlier should upgrade to one of the above patched versions. For additional details on this attack vector, please refer to https://codahale.com/a-lesson-in-timing-attacks/ .	7.4	More Details
CVE-2024-23813	A vulnerability has been identified in Polarion ALM (All versions < V2404.0). The REST API endpoints of doorsconnector of the affected product lacks proper authentication. An unauthenticated attacker could access the endpoints, and potentially execute code.	7.3	More Details
CVE-2024-24806	libuv is a multi-platform support library with a focus on asynchronous I/O. The `uv_getaddrinfo` function in `src/unix/getaddrinfo.c` (and its windows counterpart `src/win/getaddrinfo.c`), truncates hostnames to 256 characters before calling `getaddrinfo`. This behavior can be exploited to create addresses like `0x00007f000001`, which are considered valid by `getaddrinfo` and could allow an attacker to craft payloads that resolve to unintended IP addresses, bypassing developer checks. The vulnerability arises due to how the `hostname_ascii` variable (with a length of 256 bytes) is handled in `uv_getaddrinfo` and subsequently in `uv__idna_toascii`. When the hostname exceeds 256 characters, it gets truncated without a terminating null byte. As a result attackers may be able to access internal APIs or for websites (similar to MySpace) that allows users to have `username.example.com` pages. Internal services that crawl or cache these user pages can be exposed to SSRF attacks if a malicious user chooses a long vulnerable username. This issue has been addressed in release version 1.48.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23769	Improper privilege control for the named pipe in Samsung Magician PC Software 8.0.0 (for Windows) allows a local attacker to read privileged data.	7.3	More Details
CVE-2024-21329	Azure Connected Machine Agent Elevation of Privilege Vulnerability	7.3	More Details
CVE-2024-0242	Under certain circumstances IQ Panel4 and IQ4 Hub panel software prior to version 4.4.2 could allow unauthorized access to settings.	7.3	More Details
CVE-2023-38960	Insecure Permissions issue in Raiden Professional Server RaidenFTPD v.2.4 build 4005 allows a local attacker to gain privileges and execute arbitrary code via crafted executable running from the installation directory.	7.3	More Details
CVE-2024-22445	Dell PowerProtect Data Manager, version 19.15 and prior versions, contain an OS command injection vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker.	7.2	More Details
CVE-2024-0566	The Smart Manager WordPress plugin before 8.28.0 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin.	7.2	More Details
CVE-2023-6294	The Popup Builder WordPress plugin before 4.2.6 does not validate a parameter before making a request to it, which could allow users with the administrator role to perform SSRF attack in Multisite WordPress configurations.	7.2	More Details
CVE-2024-21402	Microsoft Outlook Elevation of Privilege Vulnerability	7.1	More Details
CVE-2024-25122	sidekiq-unique-jobs is an open source project which prevents simultaneous Sidekiq jobs with the same unique arguments to run. Specially crafted GET request parameters handled by any of the following endpoints of sidekiq-unique-jobs' "admin" web UI, allow a super-user attacker, or an unwitting, but authorized, victim, who has received a disguised / crafted link, to successfully execute malicious code, which could potentially steal cookies, session data, or local storage data from the app the sidekiq-unique-jobs web UI is mounted in. 1. `/changelogs`, 2. `/locks` or 3. `/expiring_locks`. This issue has been addressed in versions 7.1.33 and 8.0.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.1	More Details
CVE-2023-51488	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic, Inc. Crowdsignal Dashboard – Polls, Surveys & more allows Reflected XSS.This issue affects Crowdsignal Dashboard – Polls, Surveys & more: from n/a through 3.0.11.	7.1	More Details
CVE-2024-24879	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Yannick Lefebvre Link Library allows Reflected XSS.This issue affects Link Library: from n/a through 7.5.13.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24881	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VeronaLabs WP SMS – Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc allows Reflected XSS.This issue affects WP SMS – Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc: from n/a through 6.5.2.	7.1	More Details
CVE-2024-24877	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Magic Hills Pty Ltd Wonder Slider Lite allows Reflected XSS.This issue affects Wonder Slider Lite: from n/a through 13.9.	7.1	More Details
CVE-2024-24878	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PT Woo Plugins (by Webdados) Portugal CTT Tracking for WooCommerce allows Reflected XSS.This issue affects Portugal CTT Tracking for WooCommerce: from n/a through 2.1.	7.1	More Details
CVE-2024-24933	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Prasidhda Malla Honeypot for WP Comment allows Reflected XSS.This issue affects Honeypot for WP Comment: from n/a through 2.2.3.	7.1	More Details
CVE-2024-24932	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Djo VK Poster Group allows Reflected XSS.This issue affects VK Poster Group: from n/a through 2.0.3.	7.1	More Details
CVE-2024-24927	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UnitedThemes Brooklyn	Creative Multi-Purpose Responsive WordPress Theme allows Reflected XSS.This issue affects Brooklyn	Creative Multi-Purpose Responsive WordPress Theme: from n/a through 4.9.7.6.	7.1	More Details
CVE-2024-1163	The attacker may exploit a path traversal vulnerability leading to information disclosure.	7.1	More Details
CVE-2023-41704	Processing of CID references at E-Mail can be abused to inject malicious script code that passes the sanitization engine. Malicious script code could be injected to a users sessions when interacting with E-Mails. Please deploy the provided updates and patch releases. CID handing has been improved and resulting content is checked for malicious content. No publicly available exploits are known.	7.1	More Details
CVE-2024-25121	TYPO3 is an open source PHP based web content management system released under the GNU GPL. In affected versions of TYPO3 entities of the File Abstraction Layer (FAL) could be persisted directly via `DataHandler`. This allowed attackers to reference files in the fallback storage directly and retrieve their file names and contents. The fallback storage ("zero-storage") is used as a backward compatibility layer for files located outside properly configured file storages and within the public web root directory. Exploiting this vulnerability requires a valid backend user account. Users are advised to update to TYPO3 version 8.7.57 ELTS, 9.5.46 ELTS, 10.4.43 ELTS, 11.5.35 LTS, 12.4.11 LTS, or 13.0.1 which fix the problem described. When persisting entities of the File Abstraction Layer directly via DataHandler, `sys_file` entities are now denied by default, and `sys_file_reference` & `sys_file_metadata` entities are not permitted to reference files in the fallback storage anymore. When importing data from secure origins, this must be explicitly enabled in the corresponding DataHandler instance by using `$dataHandler->isImporting = true;`.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21405	Microsoft Message Queuing (MSMQ) Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-21355	Microsoft Message Queuing (MSMQ) Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-21371	Windows Kernel Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-22795	Insecure Permissions vulnerability in Forescout SecureConnector v.11.3.06.0063 allows a local attacker to escalate privileges via the Recheck Compliance Status component.	7.0	More Details
CVE-2023-43609	In Emerson Rosemount GC370XA, GC700XA, and GC1500XA products, an unauthenticated user with network access could obtain access to sensitive information or cause a denial-of-service condition.	6.9	More Details
CVE-2023-49716	In Emerson Rosemount GC370XA, GC700XA, and GC1500XA products, an authenticated user with network access could run arbitrary commands from a remote computer.	6.9	More Details
CVE-2024-21381	Microsoft Azure Active Directory B2C Spoofing Vulnerability	6.8	More Details
CVE-2024-21341	Windows Kernel Remote Code Execution Vulnerability	6.8	More Details
CVE-2024-23764	Certain WithSecure products allow Local Privilege Escalation. This affects WithSecure Client Security 15 and later, WithSecure Server Security 15 and later, WithSecure Email and Server Security 15 and later, and WithSecure Elements Endpoint Protection 17 and later.	6.7	More Details
CVE-2023-6840	An issue has been discovered in GitLab EE affecting all versions from 16.4 prior to 16.6.7, 16.7 prior to 16.7.5, and 16.8 prior to 16.8.2 which allows a maintainer to change the name of a protected branch that bypasses the security policy added to block MR.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24828	pkg is tool design to bundle Node.js projects into an executables. Any native code packages built by `pkg` are written to a hardcoded directory. On unix systems, this is `/tmp/pkg/*` which is a shared directory for all users on the same local system. There is no uniqueness to the package names within this directory, they are predictable. An attacker who has access to the same local system has the ability to replace the genuine executables in the shared directory with malicious executables of the same name. A user may then run the malicious executable without realising it has been modified. This package is deprecated. Therefore, there will not be a patch provided for this vulnerability. To check if your executable build by pkg depends on native code and is vulnerable, run the executable and check if `/tmp/pkg/` was created. Users should transition to actively maintained alternatives. We would recommend investigating Node.js 21's support for single executable applications. Given the decision to deprecate the pkg package, there are no official workarounds or remediations provided by our team. Users should prioritize migrating to other packages that offer similar functionality with enhanced security.	6.6	More Details
CVE-2023-41705	Processing of user-defined DAV user-agent strings is not limited. Availability of OX App Suite could be reduced due to high processing load. Please deploy the provided updates and patch releases. Processing time of DAV user-agents now gets monitored, and the related request is terminated if a resource threshold is reached. No publicly available exploits are known.	6.5	More Details
CVE-2023-41706	Processing time of drive search expressions now gets monitored, and the related request is terminated if a resource threshold is reached. Availability of OX App Suite could be reduced due to high processing load. Please deploy the provided updates and patch releases. Processing of user-defined drive search expressions is not limited No publicly available exploits are known.	6.5	More Details
CVE-2023-41707	Processing of user-defined mail search expressions is not limited. Availability of OX App Suite could be reduced due to high processing load. Please deploy the provided updates and patch releases. Processing time of mail search expressions now gets monitored, and the related request is terminated if a resource threshold is reached. No publicly available exploits are known.	6.5	More Details
CVE-2023-6564	An issue has been discovered in GitLab EE Premium and Ultimate affecting versions 16.4.3, 16.5.3, and 16.6.1. In projects using subgroups to define who can push and/or merge to protected branches, there may have been instances in which subgroup members with the Developer role were able to push or merge to protected branches.	6.5	More Details
CVE-2024-1309	Uncontrolled Resource Consumption vulnerability in Honeywell Niagara Framework on Windows, Linux, QNX allows Content Spoofing.This issue affects Niagara Framework: before Niagara AX 3.8.1, before Niagara 4.1.	6.5	More Details
CVE-2024-24871	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Creative Themes Blocksy allows Stored XSS.This issue affects Blocksy: from n/a through 2.0.19.	6.5	More Details
CVE-2024-24836	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Audrasjb GDPR Data Request Form allows Stored XSS.This issue affects GDPR Data Request Form: from n/a through 1.6.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21356	Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability	6.5	More Details
CVE-2024-24880	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apollo13Themes Apollo13 Framework Extensions allows Stored XSS.This issue affects Apollo13 Framework Extensions: from n/a through 1.9.2.	6.5	More Details
CVE-2023-51403	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nicdark Restaurant Reservations allows Stored XSS.This issue affects Restaurant Reservations: from n/a through 1.8.	6.5	More Details
CVE-2024-25109	ManageWiki is a MediaWiki extension allowing users to manage wikis. Special:ManageWiki does not escape escape interface messages on the `columns` and `help` keys on the form descriptor. An attacker may exploit this and would have a cross site scripting attack vector. Exploiting this on-wiki requires the `(editinterface)` right. Users should apply the code changes in commits `886cc6b94`, `2ef0f50880`, and `6942e8b2c` to resolve this vulnerability. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2024-24713	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Auto Listings Auto Listings – Car Listings & Car Dealership Plugin for WordPress allows Stored XSS.This issue affects Auto Listings – Car Listings & Car Dealership Plugin for WordPress: from n/a through 2.6.5.	6.5	More Details
CVE-2024-22332	The IBM Integration Bus for z/OS 10.1 through 10.1.0.2 AdminAPI is vulnerable to a denial of service due to file system exhaustion. IBM X-Force ID: 279972.	6.5	More Details
CVE-2024-25679	In PQUIC before 5bde5bb, retention of unused initial encryption keys allows attackers to disrupt a connection with a PSK configuration by sending a CONNECTION_CLOSE frame that is encrypted via the initial key computed. Network traffic sniffing is needed as part of exploitation.	6.5	More Details
CVE-2023-6815	Incorrect Privilege Assignment vulnerability in Mitsubishi Electric Corporation MELSEC iQ-R Series Safety CPU R08/16/32/120SFCPU all versions and MELSEC iQ-R Series SIL2 Process CPU R08/16/32/120PSFCPU all versions allows a remote authenticated attacker who has logged into the product as a non-administrator user to disclose the credentials (user ID and password) of a user with a lower access level than the attacker by sending a specially crafted packet.	6.5	More Details
CVE-2024-23446	An issue was discovered by Elastic, whereby the Detection Engine Search API does not respect Document-level security (DLS) or Field-level security (FLS) when querying the .alerts-security.alerts-{space_id} indices. Users who are authorized to call this API may obtain unauthorized access to documents if their roles are configured with DLS or FLS against the aforementioned index.	6.5	More Details
CVE-2023-49339	Ellucian Banner 9.17 allows Insecure Direct Object Reference (IDOR) via a modified bannerId to the /StudentSelfService/ssb/studentCard/retrieveData endpoint.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48363	A vulnerability has been identified in OpenPCS 7 V9.1 (All versions < V9.1 SP2 UC05), SIMATIC BATCH V9.1 (All versions < V9.1 SP2 UC05), SIMATIC PCS 7 V9.1 (All versions < V9.1 SP2 UC05), SIMATIC Route Control V9.1 (All versions < V9.1 SP2 UC05), SIMATIC WinCC Runtime Professional V18 (All versions < V18 Update 4), SIMATIC WinCC Runtime Professional V19 (All versions < V19 Update 2), SIMATIC WinCC V7.4 (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 15), SIMATIC WinCC V8.0 (All versions < V8.0 Update 4). The implementation of the RPC (Remote Procedure call) communication protocol in the affected products do not properly handle certain unorganized RPC messages. An attacker could use this vulnerability to cause a denial of service condition in the RPC server.	6.5	More Details
CVE-2023-48364	A vulnerability has been identified in OpenPCS 7 V9.1 (All versions < V9.1 SP2 UC05), SIMATIC BATCH V9.1 (All versions < V9.1 SP2 UC05), SIMATIC PCS 7 V9.1 (All versions < V9.1 SP2 UC05), SIMATIC Route Control V9.1 (All versions < V9.1 SP2 UC05), SIMATIC WinCC Runtime Professional V18 (All versions < V18 Update 4), SIMATIC WinCC Runtime Professional V19 (All versions < V19 Update 2), SIMATIC WinCC V7.4 (All versions), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 15), SIMATIC WinCC V8.0 (All versions < V8.0 Update 4). The implementation of the RPC (Remote Procedure call) communication protocol in the affected products do not properly handle certain malformed RPC messages. An attacker could use this vulnerability to cause a denial of service condition in the RPC server.	6.5	More Details
CVE-2024-1084	Cross-site Scripting in the tag name pattern field in the tag protections UI in GitHub Enterprise Server allows a malicious website that requires user interaction and social engineering to make changes to a user account via CSP bypass with created CSRF tokens. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in all versions of 3.11.5, 3.10.7, 3.9.10, and 3.8.15. This vulnerability was reported via the GitHub Bug Bounty program.	6.5	More Details
CVE-2024-1250	An issue has been discovered in GitLab EE affecting all versions starting from 16.8 before 16.8.2. When a user is assigned a custom role with manage_group_access_tokens permission, they may be able to create group access tokens with Owner privileges, which may lead to privilege escalation.	6.5	More Details
CVE-2024-25143	The Document and Media widget In Liferay Portal 7.2.0 through 7.3.6, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 13, and older unsupported versions, does not limit resource consumption when generating a preview image, which allows remote authenticated users to cause a denial of service (memory consumption) via crafted PNG images.	6.5	More Details
CVE-2024-24822	Pimcore's Admin Classic Bundle provides a backend user interface for Pimcore. Prior to version 1.3.3, an attacker can create, delete etc. tags without having the permission to do so. A fix is available in version 1.3.3. As a workaround, one may apply the patch manually.	6.5	More Details
CVE-2024-25451	Bento4 v1.6.0-640 was discovered to contain an out-of-memory bug via the AP4_DataBuffer::ReallocateBuffer() function.	6.5	More Details
CVE-2023-6356	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to send a set of crafted TCP packages when using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver and causing kernel panic and a denial of service.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6535	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to send a set of crafted TCP packages when using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver, causing kernel panic and a denial of service.	6.5	More Details
CVE-2023-6536	A flaw was found in the Linux kernel's NVMe driver. This issue may allow an unauthenticated malicious actor to send a set of crafted TCP packages when using NVMe over TCP, leading the NVMe driver to a NULL pointer dereference in the NVMe driver, causing kernel panic and a denial of service.	6.5	More Details
CVE-2023-6736	An issue has been discovered in GitLab EE affecting all versions starting from 11.3 before 16.7.6, all versions starting from 16.8 before 16.8.3, all versions starting from 16.9 before 16.9.1. It was possible for an attacker to cause a client-side denial of service using malicious crafted content in the CODEOWNERS file.	6.5	More Details
CVE-2024-1066	An issue has been discovered in GitLab EE affecting all versions from 13.3.0 prior to 16.6.7, 16.7 prior to 16.7.5, and 16.8 prior to 16.8.2 which allows an attacker to do a resource exhaustion using GraphQL `vulnerabilitiesCountByDay`	6.5	More Details
CVE-2023-50875	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic Sensei LMS – Online Courses, Quizzes, & Learning allows Stored XSS.This issue affects Sensei LMS – Online Courses, Quizzes, & Learning: from n/a through 4.17.0.	6.5	More Details
CVE-2024-1439	Inadequate access control in Moodle LMS. This vulnerability could allow a local user with a student role to create arbitrary events intended for users with higher roles. It could also allow the attacker to add events to the calendar of all users without their prior consent.	6.5	More Details
CVE-2024-24931	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in swadeshswain Before After Image Slider WP allows Stored XSS.This issue affects Before After Image Slider WP: from n/a through 2.2.	6.5	More Details
CVE-2024-21875	Allocation of Resources Without Limits or Throttling vulnerability in Badge leading to a denial of service attack.Team Hacker Hotel Badge 2024 on risc-v (billboard modules) allows Flooding.This issue affects Hacker Hotel Badge 2024: from 0.1.0 through 0.1.3.	6.5	More Details
CVE-2024-24801	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LogicHunt OWL Carousel – WordPress Owl Carousel Slider allows Stored XSS.This issue affects OWL Carousel – WordPress Owl Carousel Slider: from n/a through 1.4.0.	6.5	More Details
CVE-2024-24803	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPoperation Ultra Companion – Companion plugin for WPoperation Themes allows Stored XSS.This issue affects Ultra Companion – Companion plugin for WPoperation Themes: from n/a through 1.1.9.	6.5	More Details
CVE-2024-24804	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in websoudan MW WP Form allows Stored XSS.This issue affects MW WP Form: from n/a through 5.0.6.	6.5	More Details
CVE-2024-24831	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Leap13 Premium Addons for Elementor allows Stored XSS.This issue affects Premium Addons for Elementor: from n/a through 4.10.16.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51404	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MyAgilePrivacy My Agile Privacy – The only GDPR solution for WordPress that you can truly trust allows Stored XSS.This issue affects My Agile Privacy – The only GDPR solution for WordPress that you can truly trust: from n/a through 2.1.7.	6.5	More Details
CVE-2023-51415	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GiveWP GiveWP – Donation Plugin and Fundraising Platform allows Stored XSS.This issue affects GiveWP – Donation Plugin and Fundraising Platform: from n/a through 3.2.2.	6.5	More Details
CVE-2023-51480	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in realmag777 Active Products Tables for WooCommerce. Professional products tables for WooCommerce store allows Stored XSS.This issue affects Active Products Tables for WooCommerce. Professional products tables for WooCommerce store : from n/a through 1.0.6.	6.5	More Details
CVE-2023-51485	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Hosting Pay with Vipps and MobilePay for WooCommerce allows Stored XSS.This issue affects Pay with Vipps and MobilePay for WooCommerce: from n/a through 1.14.13.	6.5	More Details
CVE-2024-24712	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Team Heateor Heateor Social Login WordPress allows Stored XSS.This issue affects Heateor Social Login WordPress: from n/a through 1.1.30.	6.5	More Details
CVE-2023-51492	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in If So Plugin If-So Dynamic Content Personalization allows Stored XSS.This issue affects If-So Dynamic Content Personalization: from n/a through 1.6.3.1.	6.5	More Details
CVE-2023-51493	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Howard Ehrenberg Custom Post Carousels with Owl allows Stored XSS.This issue affects Custom Post Carousels with Owl: from n/a through 1.4.6.	6.5	More Details
CVE-2024-23514	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ClickToTweet.Com Click To Tweet allows Stored XSS.This issue affects Click To Tweet: from n/a through 2.0.14.	6.5	More Details
CVE-2024-23516	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Calculators World CC BMI Calculator allows Stored XSS.This issue affects CC BMI Calculator: from n/a through 2.0.1.	6.5	More Details
CVE-2024-23517	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Start Booking Scheduling Plugin – Online Booking for WordPress allows Stored XSS.This issue affects Scheduling Plugin – Online Booking for WordPress: from n/a through 3.5.10.	6.5	More Details
CVE-2023-32341	IBM Sterling B2B Integrator 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.3 could allow an authenticated user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 255827.	6.5	More Details
CVE-2024-20679	Azure Stack Hub Spoofing Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20684	Windows Hyper-V Denial of Service Vulnerability	6.5	More Details
CVE-2024-0971	A SQL injection vulnerability exists where an authenticated, low-privileged remote attacker could potentially alter scan DB content.	6.5	More Details
CVE-2024-24928	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Arunas Liuiza Content Cards allows Stored XSS.This issue affects Content Cards: from n/a through 0.9.7.	6.5	More Details
CVE-2023-26562	In Zimbra Collaboration (ZCS) 8.8.15 and 9.0, a closed account (with 2FA and generated passwords) can send e-mail messages when configured for Imap/smtp.	6.5	More Details
CVE-2024-24930	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OTWthemes.Com Buttons Shortcode and Widget allows Stored XSS.This issue affects Buttons Shortcode and Widget: from n/a through 1.16.	6.5	More Details
CVE-2023-5665	The Payment Forms for Paystack plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes in all versions up to, and including, 3.4.1 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. CVE-2024-32130 is likely a duplicate of this issue.	6.4	More Details
CVE-2024-0256	The Starbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Profile Display Name and Social Settings in all versions up to, and including, 3.4.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-22230	Dell Unity, versions prior to 5.4, contains a Cross-site scripting vulnerability. An authenticated attacker could potentially exploit this vulnerability, stealing session information, masquerading as the affected user or carry out any actions that this user could perform, or to generally control the victim's browser.	6.4	More Details
CVE-2024-21339	Windows USB Generic Parent Driver Remote Code Execution Vulnerability	6.4	More Details
CVE-2024-1159	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 4.8.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1353	A vulnerability, which was classified as critical, has been found in PHPEMS up to 1.0. Affected by this issue is the function index of the file app/weixin/controller/index.api.php. The manipulation of the argument picurl leads to deserialization. The exploit has been disclosed to the public and may be used. VDB-253226 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-23439	Vba32 Antivirus v3.36.0 is vulnerable to an Arbitrary Memory Read vulnerability by triggering the 0x22201B, 0x22201F, 0x222023, 0x222027 ,0x22202B, 0x22202F, 0x22203F, 0x222057 and 0x22205B IOCTL codes of the Vba32m64.sys driver.	6.3	More Details
CVE-2024-23440	Vba32 Antivirus v3.36.0 is vulnerable to an Arbitrary Memory Read vulnerability. The 0x22200B IOCTL code of the Vba32m64.sys driver allows to read up to 0x802 of memory from ar arbitrary user-supplied pointer.	6.3	More Details
CVE-2023-45187	IBM Engineering Lifecycle Optimization - Publishing 7.0.2 and 7.0.3 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 268749.	6.3	More Details
CVE-2024-1082	A path traversal vulnerability was identified in GitHub Enterprise Server that allowed an attacker to gain unauthorized read permission to files by deploying arbitrary symbolic links to a GitHub Pages site with a specially crafted artifact tarball. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.8.15, 3.9.10, 3.10.7, 3.11.5. This vulnerability was reported via the GitHub Bug Bounty program.	6.3	More Details
CVE-2024-1268	A vulnerability, which was classified as critical, was found in CodeAstro Restaurant POS System 1.0. This affects an unknown part of the file update_product.php. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-253011.	6.3	More Details
CVE-2024-1264	A vulnerability has been found in Juanpao JPShop up to 1.5.02 and classified as critical. Affected by this vulnerability is the function actionUpdate of the file /api/controllers/common/UploadsController.php. The manipulation of the argument imgage leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-253003.	6.3	More Details
CVE-2024-24739	SAP Bank Account Management (BAM) allows an authenticated user with restricted access to use functions which can result in escalation of privileges with low impact on confidentiality, integrity and availability of the application.	6.3	More Details
CVE-2024-22313	IBM Storage Defender - Resiliency Service 2.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 278749.	6.2	More Details
CVE-2023-38369	IBM Security Access Manager Container 10.0.0.0 through 10.0.6.1 does not require that docker images should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 261196.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22464	Dell EMC AppSync, versions from 4.2.0.0 to 4.6.0.0 including all Service Pack releases, contain an exposure of sensitive information vulnerability in AppSync server logs. A high privileged remote attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable system with privileges of the compromised account.	6.2	More Details
CVE-2023-45206	An issue was discovered in Zimbra Collaboration (ZCS) 8.8.15, 9.0, and 10.0. Through the help document endpoint in webmail, an attacker can inject JavaScript or HTML code that leads to cross-site scripting (XSS). (Adding an adequate message to avoid malicious code will mitigate this issue.)	6.1	More Details
CVE-2024-24130	Mail2World v12 Business Control Center was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the Usr parameter at resellercenter/login.asp.	6.1	More Details
CVE-2023-52430	The caddy-security plugin 1.1.20 for Caddy allows reflected XSS via a GET request to a URL that contains an XSS payload and begins with either a /admin or /settings/mfa/delete/ substring.	6.1	More Details
CVE-2024-24494	Cross Site Scripting vulnerability in Daily Habit Tracker v.1.0 allows a remote attacker to execute arbitrary code via the day, exercise, pray, read_book, vitamins, laundry, alcohol and meat parameters in the add-tracker.php and update-tracker.php components.	6.1	More Details
CVE-2024-24131	SuperWebMailer v9.31.0.01799 was discovered to contain a reflected cross-site scripting (XSS) vulenrability via the component api.php.	6.1	More Details
CVE-2023-41703	User ID references at mentions in document comments were not correctly sanitized. Script code could be injected to a users session when working with a malicious document. Please deploy the provided updates and patch releases. User-defined content like comments and mentions are now filtered to avoid potentially malicious content. No publicly available exploits are known.	6.1	More Details
CVE-2024-24815	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A cross-site scripting vulnerability has been discovered in the core HTML parsing module in versions of CKEditor4 prior to 4.24.0-lts. It may affect all editor instances that enabled full-page editing mode or enabled CDATA elements in Advanced Content Filtering configuration (defaults to `script` and `style` elements). The vulnerability allows attackers to inject malformed HTML content bypassing Advanced Content Filtering mechanism, which could result in executing JavaScript code. An attacker could abuse faulty CDATA content detection and use it to prepare an intentional attack on the editor. A fix is available in version 4.24.0-lts.	6.1	More Details
CVE-2023-40262	An issue was discovered in Atos Unify OpenScape Voice Trace Manager V8 before V8 R0.9.11. It allows unauthenticated Stored Cross-Site Scripting (XSS) in the administration component via Access Request.	6.1	More Details
CVE-2024-24889	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Geek Code Lab All 404 Pages Redirect to Homepage allows Stored XSS.This issue affects All 404 Pages Redirect to Homepage: from n/a through 1.9.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24816	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A cross-site scripting vulnerability vulnerability has been discovered in versions prior to 4.24.0-lts in samples that use the `preview` feature. All integrators that use these samples in the production code can be affected. The vulnerability allows an attacker to execute JavaScript code by abusing the misconfigured preview feature. It affects all users using the CKEditor 4 at version < 4.24.0-lts with affected samples used in a production environment. A fix is available in version 4.24.0-lts.	6.1	More Details
CVE-2023-49101	WebAdmin in Axigen 10.3.x before 10.3.3.61, 10.4.x before 10.4.24, and 10.5.x before 10.5.10 allows XSS attacks against admins because of mishandling of viewing the usage of SSL certificates.	6.1	More Details
CVE-2024-24034	Setor Informatica S.I.L version 3.0 is vulnerable to Open Redirect via the hprinter parameter, allows remote attackers to execute arbitrary code.	6.1	More Details
CVE-2023-51630	Paessler PRTG Network Monitor Cross-Site Scripting Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of Paessler PRTG Network Monitor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the web console. The issue results from the lack of proper validation of user-supplied data, which can lead to the injection of an arbitrary script. An attacker can leverage this vulnerability to bypass authentication on the system. . Was ZDI-CAN-21182.	6.1	More Details
CVE-2024-0250	The Analytics Insights for Google Analytics 4 (AIWP) WordPress plugin before 6.3 is vulnerable to Open Redirect due to insufficient validation on the redirect oauth2callback.php file. This makes it possible for unauthenticated attackers to redirect users to potentially malicious sites if they can successfully trick them into performing an action.	6.1	More Details
CVE-2024-25715	Glewlwyd SSO server 2.x through 2.7.6 allows open redirection via redirect_uri.	6.1	More Details
CVE-2023-45207	An issue was discovered in Zimbra Collaboration (ZCS) 8.8.15, 9.0, and 10.0. An attacker can send a PDF document through mail that contains malicious JavaScript. While previewing this file in webmail in the Chrome browser, the stored XSS payload is executed. (This has been mitigated by sanitising the JavaScript code present in a PDF document.)	6.1	More Details
CVE-2023-50808	Zimbra Collaboration before Kepler 9.0.0 Patch 38 GA allows DOM-based JavaScript injection in the Modern UI.	6.1	More Details
CVE-2023-39683	Cross Site Scripting (XSS) vulnerability in EasyEmail v.4.12.2 and before allows a local attacker to execute arbitrary code via the user input parameter(s). NOTE: Researcher claims issue is present in all versions prior and later than tested version.	6.1	More Details
CVE-2023-48432	An issue was discovered in Zimbra Collaboration (ZCS) 8.8.15, 9.0, and 10.0. XSS, with resultant session stealing, can occur via JavaScript code in a link (for a webmail redirection endpoint) within en email message, e.g., if a victim clicks on that link within Zimbra webmail.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1037	The All-In-One Security (AIOS) – Security and Firewall plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 5.2.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-31346	Failure to initialize memory in SEV Firmware may allow a privileged attacker to access stale data from other guests.	6.0	More Details
CVE-2023-7169	Authentication Bypass by Spoofing vulnerability in Snow Software Snow Inventory Agent on Windows allows Signature Spoof.This issue affects Snow Inventory Agent: through 6.14.5. Customers advised to upgrade to version 7.0	6.0	More Details
CVE-2023-20579	Improper Access Control in the AMD SPI protection feature may allow a user with Ring0 (kernel mode) privileged access to bypass protections potentially resulting in loss of integrity and availability.	6.0	More Details
CVE-2024-21491	Versions of the package svix before 1.17.0 are vulnerable to Authentication Bypass due to an issue in the verify function where signatures of different lengths are incorrectly compared. An attacker can bypass signature verification by providing a shorter signature that matches the beginning of the actual signature. **Note:** The attacker would need to know a victim uses the Rust library for verification,no easy way to automatically check that; and uses webhooks by a service that uses Svix, and then figure out a way to craft a malicious payload that will actually include all of the correct identifiers needed to trick the receivers to cause actual issues.	5.9	More Details
CVE-2023-51370	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NinjaTeam WP Chat App allows Stored XSS.This issue affects WP Chat App: from n/a through 3.4.4.	5.9	More Details
CVE-2024-21343	Windows Network Address Translation (NAT) Denial of Service Vulnerability	5.9	More Details
CVE-2023-6935	wolfSSL SP Math All RSA implementation is vulnerable to the Marvin Attack, new variation of a timing Bleichenbacher style attack, when built with the following options to configure: --enable-all CFLAGS="-DWOLFSSL_STATIC_RSA" The define “WOLFSSL_STATIC_RSA” enables static RSA cipher suites, which is not recommended, and has been disabled by default since wolfSSL 3.6.6. Therefore the default build since 3.6.6, even with "--enable-all", is not vulnerable to the Marvin Attack. The vulnerability is specific to static RSA cipher suites, and expected to be padding-independent. The vulnerability allows an attacker to decrypt ciphertexts and forge signatures after probing with a large number of test observations. However the server’s private key is not exposed.	5.9	More Details
CVE-2023-47526	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chart Builder Team Chartify – WordPress Chart Plugin allows Stored XSS.This issue affects Chartify – WordPress Chart Plugin: from n/a through 2.0.6.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50349	Sametime is impacted by a Cross Site Request Forgery (CSRF) vulnerability. Some REST APIs in the Sametime Proxy application can allow an attacker to perform malicious actions on the application.	5.9	More Details
CVE-2022-34310	IBM CICS TX Standard and Advanced 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 229441.	5.9	More Details
CVE-2024-24834	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in realmag777 BEAR – Bulk Editor and Products Manager Professional for WooCommerce by Pluginus.Net allows Stored XSS.This issue affects BEAR – Bulk Editor and Products Manager Professional for WooCommerce by Pluginus.Net: from n/a through 1.1.4.	5.9	More Details
CVE-2023-47700	IBM SAN Volume Controller, IBM Storwize, IBM FlashSystem and IBM Storage Virtualize 8.6 products could allow a remote attacker to spoof a trusted system that would not be correctly validated by the Storwize server. This could lead to a user connecting to a malicious host, believing that it was a trusted system and deceived into accepting spoofed data. IBM X-Force ID: 271016.	5.9	More Details
CVE-2024-24717	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mark Kinchin Beds24 Online Booking allows Stored XSS.This issue affects Beds24 Online Booking: from n/a through 2.0.23.	5.9	More Details
CVE-2024-22361	IBM Semeru Runtime 8.0.302.0 through 8.0.392.0, 11.0.12.0 through 11.0.21.0, 17.0.1.0 - 17.0.9.0, and 21.0.1.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 281222.	5.9	More Details
CVE-2024-24885	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Lê Văn Toản Woocommerce Vietnam Checkout allows Stored XSS.This issue affects Woocommerce Vietnam Checkout: from n/a through 2.0.7.	5.9	More Details
CVE-2024-24886	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Acowebs Product Labels For Woocommerce (Sale Badges) allows Stored XSS.This issue affects Product Labels For Woocommerce (Sale Badges): from n/a through 1.5.3.	5.9	More Details
CVE-2022-34309	IBM CICS TX Standard and Advanced 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 229440.	5.9	More Details
CVE-2024-21344	Windows Network Address Translation (NAT) Denial of Service Vulnerability	5.9	More Details
CVE-2023-50358	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later QTS 4.5.4.2627 build 20231225 and later QTS 4.3.6.2665 build 20240131 and later QTS 4.3.4.2675 build 20240131 and later QTS 4.3.3.2644 build 20240131 and later QTS 4.2.6 build 20240131 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1140	Twister Antivirus v8.17 is vulnerable to an Out-of-bounds Read vulnerability by triggering the 0x801120B8 IOCTL code of the filmfd.sys driver.	5.8	More Details
CVE-2023-47218	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.5.2645 build 20240116 and later QuTS hero h5.1.5.2647 build 20240118 and later QuTScloud c5.1.5.2651 and later	5.8	More Details
CVE-2024-21624	nonebot2 is a cross-platform Python asynchronous chatbot framework written in Python. This security advisory pertains to a potential information leak (e.g., environment variables) in instances where developers utilize `MessageTemplate` and incorporate user-provided data into templates. The identified vulnerability has been remedied in pull request #2509 and will be included in versions released from 2.2.0. Users are strongly advised to upgrade to these patched versions to safeguard against the vulnerability. A temporary workaround involves filtering underscores before incorporating user input into the message template.	5.7	More Details
CVE-2024-23448	An issue was discovered whereby APM Server could log at ERROR level, a response from Elasticsearch indicating that indexing the document failed and that response would contain parts of the original document. Depending on the nature of the document that the APM Server attempted to ingest, this could lead to the insertion of sensitive or private information in the APM Server logs.	5.7	More Details
CVE-2024-20695	Skype for Business Information Disclosure Vulnerability	5.7	More Details
CVE-2024-0169	Dell Unity, version(s) 5.3 and prior, contain(s) an Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	5.7	More Details
CVE-2024-24823	Graylog is a free and open log management platform. Starting in version 4.3.0 and prior to versions 5.1.11 and 5.2.4, reauthenticating with an existing session cookie would re-use that session id, even if for different user credentials. In this case, the pre-existing session could be used to gain elevated access to an existing Graylog login session, provided the malicious user could successfully inject their session cookie into someone else's browser. The complexity of such an attack is high, because it requires presenting a spoofed login screen and injection of a session cookie into an existing browser, potentially through a cross-site scripting attack. No such attack has been discovered. Graylog 5.1.11 and 5.2.4, and any versions of the 6.0 development branch, contain patches to not re-use sessions under any circumstances. Some workarounds are available. Using short session expiration and explicit log outs of unused sessions can help limiting the attack vector. Unpatched this vulnerability exists, but is relatively hard to exploit. A proxy could be leveraged to clear the `authentication` cookie for the Graylog server URL for the `/api/system/sessions` endpoint, as that is the only one vulnerable.	5.7	More Details
CVE-2024-21377	Windows DNS Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21362	Windows Kernel Security Feature Bypass Vulnerability	5.5	More Details
CVE-2024-1096	Twister Antivirus v8.17 is vulnerable to a Denial of Service vulnerability by triggering the 0x80112067, 0x801120CB 0x801120CC 0x80112044, 0x8011204B, 0x8011204F, 0x80112057, 0x8011205B, 0x8011205F, 0x80112063, 0x8011206F, 0x80112073, 0x80112077, 0x80112078, 0x8011207C and 0x80112080 IOCTL codes of the fildds.sys driver.	5.5	More Details
CVE-2024-25740	A memory leak flaw was found in the UBI driver in drivers/mtd/ubi/attach.c in the Linux kernel through 6.7.4 for UBI_IOCATT, because kobj->name is not released.	5.5	More Details
CVE-2024-25454	Bento4 v1.6.0-640 was discovered to contain a NULL pointer dereference via the AP4_DescriptorFinder::Test() function.	5.5	More Details
CVE-2023-52429	dm_table_create in drivers/md/dm-table.c in the Linux kernel through 6.7.4 can attempt to (in alloc_targets) allocate more than INT_MAX bytes, and crash, because of a missing check for struct dm_ioctl.target_count.	5.5	More Details
CVE-2024-24488	An issue in Shenzen Tenda Technology CP3V2.0 V11.10.00.2311090948 allows a local attacker to obtain sensitive information via the password component.	5.5	More Details
CVE-2024-1062	A heap overflow flaw was found in 389-ds-base. This issue leads to a denial of service when writing a value larger than 256 chars in log_entry_attr.	5.5	More Details
CVE-2023-28018	HCL Connections is vulnerable to a denial of service, caused by improper validation on certain requests. Using a specially-crafted request an attacker could exploit this vulnerability to cause denial of service for affected users.	5.5	More Details
CVE-2024-25739	create_empty_lvol in drivers/mtd/ubi/vtbl.c in the Linux kernel through 6.7.4 can attempt to allocate zero bytes, and crash, because of a missing check for ubi->leb_size.	5.5	More Details
CVE-2024-24826	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 version v0.28.1. The vulnerable function, `QuickTimeVideo::NikonTagsDecoder`, was new in v0.28.0, so Exiv2 versions before v0.28 are _not_ affected. The out-of-bounds read is triggered when Exiv2 is used to read the metadata of a crafted video file. In most cases this out of bounds read will result in a crash. This bug is fixed in version v0.28.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25112	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A denial-of-service was found in Exiv2 version v0.28.1: an unbounded recursion can cause Exiv2 to crash by exhausting the stack. The vulnerable function, `QuickTimeVideo::multipleEntriesDecoder`, was new in v0.28.0, so Exiv2 versions before v0.28 are _not_ affected. The denial-of-service is triggered when Exiv2 is used to read the metadata of a crafted video file. This bug is fixed in version v0.28.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.5	More Details
CVE-2024-25741	printer_write in drivers/usb/gadget/function/f_printer.c in the Linux kernel through 6.7.4 does not properly call usb_ep_queue, which might allow attackers to cause a denial of service or have unspecified other impact.	5.5	More Details
CVE-2024-0849	Leanote version 2.7.0 allows obtaining arbitrary local files. This is possible because the application is vulnerable to LFR.	5.5	More Details
CVE-2024-1151	A vulnerability was reported in the Open vSwitch sub-component in the Linux Kernel. The flaw occurs when a recursive operation of code push recursively calls into the code block. The OVS module does not validate the stack depth, pushing too many frames and causing a stack overflow. As a result, this can lead to a crash or other related issues.	5.5	More Details
CVE-2024-25453	Bento4 v1.6.0-640 was discovered to contain a NULL pointer dereference via the AP4_StszAtom::GetSampleSize() function.	5.5	More Details
CVE-2024-25452	Bento4 v1.6.0-640 was discovered to contain an out-of-memory bug via the AP4_UrlAtom::AP4_UrlAtom() function.	5.5	More Details
CVE-2024-22119	The cause of vulnerability is improper validation of form input field “Name” on Graph page in Items section.	5.5	More Details
CVE-2024-0420	The MapPress Maps for WordPress plugin before 2.88.15 does not sanitize and escape the map title when outputting it back in the admin dashboard, allowing Contributors and above roles to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-41708	References to the "app loader" functionality could contain redirects to unexpected locations. Attackers could forge app references that bypass existing safeguards to inject malicious script code. Please deploy the provided updates and patch releases. References to apps are now controlled more strict to avoid relative references. No publicly available exploits are known.	5.4	More Details
CVE-2023-46615	Deserialization of Untrusted Data vulnerability in Kalli Dan. KD Coming Soon.This issue affects KD Coming Soon: from n/a through 1.7.	5.4	More Details
CVE-2024-24115	A stored cross-site scripting (XSS) vulnerability in the Edit Page function of Cotonti CMS v0.9.24 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24887	Cross-Site Request Forgery (CSRF) vulnerability in Contest Gallery Photos and Files Contest Gallery – Contact Form, Upload Form, Social Share and Voting Plugin for WordPress.This issue affects Photos and Files Contest Gallery – Contact Form, Upload Form, Social Share and Voting Plugin for WordPress: from n/a through 21.2.8.4.	5.4	More Details
CVE-2024-1160	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Icon Link in all versions up to, and including, 4.8.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2024-1157	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's button URL in all versions up to, and including, 4.8.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2024-25148	In Liferay Portal 7.2.0 through 7.4.1, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 15, and older unsupported versions the `doAsUserId` URL parameter may get leaked when creating linked content using the WYSIWYG editor and while impersonating a user. This may allow remote authenticated users to impersonate a user after accessing the linked content.	5.4	More Details
CVE-2023-6081	The chartjs WordPress plugin through 2023.2 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).	5.4	More Details
CVE-2023-6499	The lasTunes WordPress plugin through 3.6.1 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	5.4	More Details
CVE-2023-47798	Account lockout in Liferay Portal 7.2.0 through 7.3.0, and older unsupported versions, and Liferay DXP 7.2 before fix pack 5, and older unsupported versions does not invalidate existing user sessions, which allows remote authenticated users to remain authenticated after an account has been locked.	5.4	More Details
CVE-2023-31506	A cross-site scripting (XSS) vulnerability in Grav versions 1.7.44 and before, allows remote authenticated attackers to execute arbitrary web scripts or HTML via the onmouseover attribute of an ISINDEX element.	5.4	More Details
CVE-2024-24706	Cross-Site Request Forgery (CSRF) vulnerability in Forum One WP-CFM wp-cfm.This issue affects WP-CFM: from n/a through 1.7.8.	5.4	More Details
CVE-2024-22129	SAP Companion - version <3.1.38, has a URL with parameter that could be vulnerable to XSS attack. The attacker could send a malicious link to a user that would possibly allow an attacker to retrieve the sensitive information and cause minor impact on the integrity of the web application.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6082	The chartjs WordPress plugin through 2023.2 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).	5.4	More Details
CVE-2023-6152	A user changing their email after signing up and verifying it can change it without verification in profile settings. The configuration option "verify_email_enabled" will only validate email only on sign up.	5.4	More Details
CVE-2024-24812	Frappe is a full-stack web application framework that uses Python and MariaDB on the server side and a tightly integrated client side library. Prior to versions 14.59.0 and 15.5.0, portal pages are susceptible to Cross-Site Scripting (XSS) which can be used to inject malicious JS code if user clicks on a malicious link. This vulnerability has been patched in versions 14.59.0 and 15.5.0. No known workarounds are available.	5.4	More Details
CVE-2023-52059	A cross-site scripting (XSS) vulnerability in Gestsup v3.2.46 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Description text field.	5.4	More Details
CVE-2024-1055	The PowerPack Addons for Elementor (Free Widgets, Extensions and Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's buttons in all versions up to, and including, 2.7.14 due to insufficient input sanitization and output escaping on user supplied URL values. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2023-40355	Cross Site Scripting (XSS) vulnerability in Axigen versions 10.3.3.0 before 10.3.3.59, 10.4.0 before 10.4.19, and 10.5.0 before 10.5.5, allows authenticated attackers to execute arbitrary code and obtain sensitive information via the logic for switching between the Standard and Ajax versions.	5.4	More Details
CVE-2024-1109	The Podlove Podcast Publisher plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the init_download() and init() functions in all versions up to, and including, 4.0.11. This makes it possible for unauthenticated attackers to export the plugin's tracking data and podcast information.	5.3	More Details
CVE-2024-0596	The Awesome Support – WordPress HelpDesk & Support Plugin plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the editor_html() function in all versions up to, and including, 6.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to view password protected and draft posts.	5.3	More Details
CVE-2024-24740	SAP NetWeaver Application Server (ABAP) - versions KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.93, KERNEL 7.94, KRNL64UC 7.53, under certain conditions, allows an attacker to access information which could otherwise be restricted with low impact on confidentiality of the application.	5.3	More Details
CVE-2024-1122	The Event Manager, Events Calendar, Events Tickets for WooCommerce – Eventin plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the export_data() function in all versions up to, and including, 3.3.50. This makes it possible for unauthenticated attackers to export event data.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24819	icingaweb2-module-incubator is a working project of bleeding edge Icinga Web 2 libraries. In affected versions the class `gipfl\Web\Form` is the base for various concrete form implementations [1] and provides protection against cross site request forgery (CSRF) by default. This is done by automatically adding an element with a CSRF token to any form, unless explicitly disabled, but even if enabled, the CSRF token (sent during a client's submission of a form relying on it) is not validated. This enables attackers to perform changes on behalf of a user which, unknowingly, interacts with a prepared link or website. The version 0.22.0 is available to remedy this issue. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2024-23447	An issue was discovered in the Windows Network Drive Connector when using Document Level Security to assign permissions to a file, with explicit allow write and deny read. Although the document is not accessible to the user in Network Drive it is visible in search applications to the user.	5.3	More Details
CVE-2024-1459	A path traversal vulnerability was found in Undertow. This issue may allow a remote attacker to append a specially-crafted sequence to an HTTP request for an application deployed to JBoss EAP, which may permit access to privileged or restricted files and directories.	5.3	More Details
CVE-2024-25360	A hidden interface in Motorola CX2L Router firmware v1.0.1 leaks information regarding the SystemWizardStatus component via sending a crafted request to device_web_ip.	5.3	More Details
CVE-2024-1079	The Quiz Maker plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the ays_show_results() function in all versions up to, and including, 6.5.2.4. This makes it possible for unauthenticated attackers to fetch arbitrary quiz results which can contain PII.	5.3	More Details
CVE-2024-24215	An issue in the component /cgi-bin/GetJsonValue.cgi of Cellinx NVT Web Server 5.0.0.014 allows attackers to leak configuration information via a crafted POST request.	5.3	More Details
CVE-2024-0421	The MapPress Maps for WordPress plugin before 2.88.16 is affected by an IDOR as it does not ensure that posts to be retrieve via an AJAX action is a public map, allowing unauthenticated users to read arbitrary private and draft posts.	5.3	More Details
CVE-2023-5680	If a resolver cache has a very large number of ECS records stored for the same name, the process of cleaning the cache database node for this name can significantly impair query performance. This issue affects BIND 9 versions 9.11.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.	5.3	More Details
CVE-2024-25146	Liferay Portal 7.2.0 through 7.4.1, and older unsupported versions, and Liferay DXP 7.3 before service pack 3, 7.2 before fix pack 18, and older unsupported versions returns with different responses depending on whether a site does not exist or if the user does not have permission to access the site, which allows remote attackers to discover the existence of sites by enumerating URLs. This vulnerability occurs if locale.prepend.friendly.url.style=2 and if a custom 404 page is used.	5.3	More Details
CVE-2024-21397	Microsoft Azure File Sync Elevation of Privilege Vulnerability	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1110	The Podlove Podcast Publisher plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the init() function in all versions up to, and including, 4.0.11. This makes it possible for unauthenticated attackers to import the plugin's settings.	5.3	More Details
CVE-2023-6681	A vulnerability was found in JWCrypto. This flaw allows an attacker to cause a denial of service (DoS) attack and possible password brute-force and dictionary attacks to be more resource-intensive. This issue can result in a large amount of computational consumption, causing a denial of service attack.	5.3	More Details
CVE-2023-39196	Improper Authentication vulnerability in Apache Ozone. The vulnerability allows an attacker to download metadata internal to the Storage Container Manager service without proper authentication. The attacker is not allowed to do any modification within the Ozone Storage Container Manager service using this vulnerability. The accessible metadata does not contain sensitive information that can be used to exploit the system later on, and the accessible data does not make it possible to gain access to actual user data within Ozone. This issue affects Apache Ozone: 1.2.0 and subsequent releases up until 1.3.0. Users are recommended to upgrade to version 1.4.0, which fixes the issue.	5.3	More Details
CVE-2024-0965	The Simple Page Access Restriction plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.21 via the REST API. This makes it possible for unauthenticated attackers to bypass the plugin's page restriction and view page content.	5.3	More Details
CVE-2024-23806	Sensitive data can be extracted from HID iCLASS SE reader configuration cards. This could include credential and device administrator keys.	5.3	More Details
CVE-2023-31002	IBM Security Access Manager Container 10.0.0.0 through 10.0.6.1 temporarily stores sensitive information in files that could be accessed by a local user. IBM X-Force ID: 254657.	5.1	More Details
CVE-2023-45190	IBM Engineering Lifecycle Optimization 7.0.2 and 7.0.3 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 268754.	5.1	More Details
CVE-2024-22318	IBM i Access Client Solutions (ACS) 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.4 is vulnerable to NT LAN Manager (NTLM) hash disclosure by an attacker modifying UNC capable paths within ACS configuration files to point to a hostile server. If NTLM is enabled, the Windows operating system will try to authenticate using the current user's session. The hostile server could capture the NTLM hash information to obtain the user's credentials. IBM X-Force ID: 279091.	5.1	More Details
CVE-2024-1312	A use-after-free flaw was found in the Linux kernel's Memory Management subsystem when a user wins two races at the same time with a fail in the mas_prev_slot function. This issue could allow a local user to crash the system.	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23639	Micronaut Framework is a modern, JVM-based, full stack Java framework designed for building modular, easily testable JVM applications with support for Java, Kotlin and the Groovy language. Enabled but unsecured management endpoints are susceptible to drive-by localhost attacks. While not typical of a production application, these attacks may have more impact on a development environment where such endpoints may be flipped on without much thought. A malicious/compromised website can make HTTP requests to `localhost`. Normally, such requests would trigger a CORS preflight check which would prevent the request; however, some requests are "simple" and do not require a preflight check. These endpoints, if enabled and not secured, are vulnerable to being triggered. Production environments typically disable unused endpoints and secure/restrict access to needed endpoints. A more likely victim is the developer in their local development host, who has enabled endpoints without security for the sake of easing development. This issue has been addressed in version 3.8.3. Users are advised to upgrade.	5.1	More Details
CVE-2023-6388	Suite CRM version 7.14.2 allows making arbitrary HTTP requests through the vulnerable server. This is possible because the application is vulnerable to SSRF.	5.0	More Details
CVE-2024-1432	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in DeepFaceLab pretrained DF.wf.288res.384.92.72.22 and classified as problematic. This issue affects the function apply_xseg of the file main.py. The manipulation leads to deserialization. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-253391. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	5.0	More Details
CVE-2024-21374	Microsoft Teams for Android Information Disclosure Vulnerability	5.0	More Details
CVE-2023-31347	Due to a code bug in Secure_TSC, SEV firmware may allow an attacker with high privileges to cause a guest to observe an incorrect TSC when Secure TSC is enabled potentially resulting in a loss of guest integrity.	4.9	More Details
CVE-2022-38714	IBM DataStage on Cloud Pak for Data 4.0.6 to 4.5.2 stores sensitive credential information that can be read by a privileged user. IBM X-Force ID: 235060.	4.9	More Details
CVE-2024-25119	TYPO3 is an open source PHP based web content management system released under the GNU GPL. The plaintext value of `$GLOBALS['SYS']['encryptionKey']` was displayed in the editing forms of the TYPO3 Install Tool user interface. This allowed attackers to utilize the value to generate cryptographic hashes used for verifying the authenticity of HTTP request parameters. Exploiting this vulnerability requires an administrator-level backend user account with system maintainer permissions. Users are advised to update to TYPO3 versions 8.7.57 ELTS, 9.5.46 ELTS, 10.4.43 ELTS, 11.5.35 LTS, 12.4.11 LTS, 13.0.1 that fix the problem described. There are no known workarounds for this vulnerability.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25107	WikiDiscover is an extension designed for use with a CreateWiki managed farm to display wikis. On Special:WikiDiscover, the `Language::date` function is used when making the human-readable timestamp for inclusion on the wiki_creation column. This function uses interface messages to translate the names of months and days. It uses the `->text()` output mode, returning unescaped interface messages. Since the output is not escaped later, the unescaped interface message is included on the output, resulting in an XSS vulnerability. Exploiting this on-wiki requires the `(editinterface)` right. This vulnerability has been addressed in commit `267e763a0`. Users are advised to update their installations. There are no known workarounds for this vulnerability.	4.9	More Details
CVE-2023-45698	Sametime is impacted by lack of clickjacking protection in Outlook add-in. The application is not implementing appropriate protections in order to protect users from clickjacking attacks.	4.8	More Details
CVE-2024-0955	A stored XSS vulnerability exists where an authenticated, remote attacker with administrator privileges on the Nessus application could alter Nessus proxy settings, which could lead to the execution of remote arbitrary scripts.	4.8	More Details
CVE-2023-6591	The Popup Box WordPress plugin before 20.9.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2023-7233	The GigPress WordPress plugin through 2.3.29 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-2024-22128	SAP NWBC for HTML - versions SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An unauthenticated attacker can inject malicious javascript to cause limited impact to confidentiality and integrity of the application data after successful exploitation.	4.7	More Details
CVE-2023-6072	A cross-site scripting vulnerability in Trellix Central Management (CM) prior to 9.1.3.97129 allows a remote authenticated attacker to craft CM dashboard internal requests causing arbitrary content to be injected into the response when accessing the CM dashboard.	4.6	More Details
CVE-2022-22506	IBM Robotic Process Automation 21.0.2 contains a vulnerability that could allow user ids may be exposed across tenants. IBM X-Force ID: 227293.	4.6	More Details
CVE-2024-21340	Windows Kernel Information Disclosure Vulnerability	4.6	More Details
CVE-2024-22221	Dell Unity, versions prior to 5.4, contains SQL Injection vulnerability. An authenticated attacker could potentially exploit this vulnerability, leading to exposure of sensitive information.	4.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0657	The Internal Link Juicer: SEO Auto Linker for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings such as 'ilj_settings_field_links_per_page' in all versions up to, and including, 2.23.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2023-28077	Dell BSAFE SSL-J, versions prior to 6.5, and versions 7.0 and 7.1 contain a debug message revealing unnecessary information vulnerability. This may lead to disclosing sensitive information to a locally privileged user.	4.4	More Details
CVE-2024-22312	IBM Storage Defender - Resiliency Service 2.0 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 278748.	4.4	More Details
CVE-2024-0977	The Timeline Widget For Elementor (Elementor Timeline, Vertical & Horizontal Timeline) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via image URLs in the plugin's timeline widget in all versions up to, and including, 1.5.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page, changes the slideshow type, and then changes it back to an image.	4.4	More Details
CVE-2023-6501	The Splashscreen WordPress plugin through 0.20 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details
CVE-2024-1078	The Quiz Maker plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ays_quick_start() and add_question_rows() functions in all versions up to, and including, 6.5.2.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to create arbitrary quizzes.	4.3	More Details
CVE-2024-24875	Cross-Site Request Forgery (CSRF) vulnerability in Yannick Lefebvre Link Library.This issue affects Link Library: from n/a through 7.5.13.	4.3	More Details
CVE-2023-40264	An issue was discovered in Atos Unify OpenScape Voice Trace Manager V8 before V8 R0.9.11. It allows authenticated path traversal in the user interface.	4.3	More Details
CVE-2023-52060	A Cross-Site Request Forgery (CSRF) in Gestsup v3.2.46 allows attackers to arbitrarily edit user profile information via a crafted request.	4.3	More Details
CVE-2024-24884	Cross-Site Request Forgery (CSRF) vulnerability in ARI Soft Contact Form 7 Connector.This issue affects Contact Form 7 Connector: from n/a through 1.2.2.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1404	A vulnerability was found in Linksys WRT54GL 4.30.18 and classified as problematic. Affected by this issue is some unknown functionality of the file /SysInfo.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-253328. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-42016	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.3 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 265559.	4.3	More Details
CVE-2024-24929	Cross-Site Request Forgery (CSRF) vulnerability in Ryan Duff, Peter Westwood WP Contact Form.This issue affects WP Contact Form: from n/a through 1.6.	4.3	More Details
CVE-2024-24935	Cross-Site Request Forgery (CSRF) vulnerability in WpSimpleTools Basic Log Viewer.This issue affects Basic Log Viewer: from n/a through 1.0.4.	4.3	More Details
CVE-2024-0511	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.87. This is due to missing or incorrect nonce validation on the wpr_update_form_action_meta function. This makes it possible for unauthenticated attackers to post metadata via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2022-34311	IBM CICS TX Standard and Advanced 11.1 could allow a user with physical access to the web browser to gain access to the user's session due to insufficiently protected credentials. IBM X-Force ID: 229446.	4.3	More Details
CVE-2024-0248	The EazyDocs WordPress plugin before 2.4.0 re-introduced CVE-2023-6029 (https://wpscan.com/vulnerability/7a0aaf85-8130-4fd7-8f09-f8edc929597e/) in 2.3.8, allowing any authenticated users, such as subscriber to delete arbitrary posts, as well as add and delete documents/sections. The issue was partially fixed in 2.3.9.	4.3	More Details
CVE-2024-24829	Sentry is an error tracking and performance monitoring platform. Sentry’s integration platform provides a way for external services to interact with Sentry. One of such integrations, the Phabricator integration (maintained by Sentry) with version <=24.1.1 contains a constrained SSRF vulnerability. An attacker could make Sentry send POST HTTP requests to arbitrary URLs (including internal IP addresses) by providing an unsanitized input to the Phabricator integration. However, the body payload is constrained to a specific format. If an attacker has access to a Sentry instance, this allows them to: 1. interact with internal network; 2. scan local/remote ports. This issue has been fixed in Sentry self-hosted release 24.1.2, and has already been mitigated on sentry.io on February 8. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24751	sf_event_mgt is an event management and registration extension for the TYPO3 CMS based on ExtBase and Fluid. In affected versions the existing access control check for events in the backend module got broken during the update of the extension to TYPO3 12.4, because the `RedirectResponse` from the `$this->redirect()` function was never handled. This issue has been addressed in version 7.4.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2024-24782	An unauthenticated attacker can send a ping request from one network to another through an error in the origin verification even though the ports are separated by VLAN.	4.3	More Details
CVE-2024-25643	The SAP Fiori app (My Overtime Request) - version 605, does not perform the necessary authorization checks for an authenticated user which may result in an escalation of privileges. It is possible to manipulate the URLs of data requests to access information that the user should not have access to. There is no impact on integrity and availability.	4.3	More Details
CVE-2024-1431	A vulnerability was found in Netgear R7000 1.0.11.136_10.2.120 and classified as problematic. Affected by this issue is some unknown functionality of the file /debuginfo.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. VDB-253382 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-23323	Envoy is a high-performance edge/middle/service proxy. The regex expression is compiled for every request and can result in high CPU usage and increased request latency when multiple routes are configured with such matchers. This issue has been addressed in released 1.29.1, 1.28.1, 1.27.3, and 1.26.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2024-1430	A vulnerability has been found in Netgear R7000 1.0.11.136_10.2.120 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /currentsetting.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-22021	Vulnerability CVE-2024-22021 allows a Veeam Recovery Orchestrator user with a low privileged role (Plan Author) to retrieve plans from a Scope other than the one they are assigned to.	4.3	More Details
CVE-2024-1406	A vulnerability was found in Linksys WRT54GL 4.30.18. It has been declared as problematic. This vulnerability affects unknown code of the file /SysInfo1.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. VDB-253330 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-25914	Cross-Site Request Forgery (CSRF) vulnerability in Photoboxone SMTP Mail.This issue affects SMTP Mail: from n/a through 1.3.20.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24741	SAP Master Data Governance for Material Data - versions 618, 619, 620, 621, 622, 800, 801, 802, 803, 804, does not perform necessary authorization check for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read some sensitive information but no impact to integrity and availability.	4.3	More Details
CVE-2024-25118	TYPO3 is an open source PHP based web content management system released under the GNU GPL. Password hashes were being reflected in the editing forms of the TYPO3 backend user interface. This allowed attackers to crack the plaintext password using brute force techniques. Exploiting this vulnerability requires a valid backend user account. Users are advised to update to TYPO3 versions 8.7.57 ELTS, 9.5.46 ELTS, 10.4.43 ELTS, 11.5.35 LTS, 12.4.11 LTS, 13.0.1 that fix the problem described. There are no known workarounds for this issue.	4.3	More Details
CVE-2024-0595	The Awesome Support – WordPress HelpDesk & Support Plugin plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the wpas_get_users() function hooked via AJAX in all versions up to, and including, 6.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve user data such as emails.	4.3	More Details
CVE-2024-1405	A vulnerability was found in Linksys WRT54GL 4.30.18. It has been classified as problematic. This affects an unknown part of the file /wlaninfo.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. The identifier VDB-253329 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-25120	TYPO3 is an open source PHP based web content management system released under the GNU GPL. The TYPO3-specific `t3://` URI scheme could be used to access resources outside of the users' permission scope. This encompassed files, folders, pages, and records (although only if a valid link-handling configuration was provided). Exploiting this vulnerability requires a valid backend user account. Users are advised to update to TYPO3 versions 8.7.57 ELTS, 9.5.46 ELTS, 10.4.43 ELTS, 11.5.35 LTS, 12.4.11 LTS, 13.0.1 that fix the problem described. There are no known workarounds for this issue.	4.3	More Details
CVE-2024-1402	Mattermost fails to check if a custom emoji reaction exists when sending it to a post and to limit the amount of custom emojis allowed to be added in a post, allowing an attacker sending a huge amount of non-existent custom emojis in a post to crash the mobile app of a user seeing the post and to crash the server due to overloading when clients attempt to retrive the aforementioned post.	4.3	More Details
CVE-2024-24742	SAP CRM WebClient UI - version S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to integrity of the application data after successful exploitation. There is no impact on confidentiality and availability.	4.1	More Details
CVE-2024-21304	Trusted Compute Base Elevation of Privilege Vulnerability	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25144	The IFrame widget in Liferay Portal 7.2.0 through 7.4.3.26, and older unsupported versions, and Liferay DXP 7.4 before update 27, 7.3 before update 6, 7.2 before fix pack 19, and older unsupported versions does not check the URL of the IFrame, which allows remote authenticated users to cause a denial-of-service (DoS) via a self referencing IFrame.	4.1	More Details
CVE-2023-45696	Sametime is impacted by sensitive fields with autocomplete enabled in the Legacy web chat client. By default, this allows user entered data to be stored by the browser.	4.0	More Details
CVE-2023-45718	Sametime is impacted by a failure to invalidate sessions. The application is setting sensitive cookie values in a persistent manner in Sametime Web clients. When this happens, cookie values can remain valid even after a user has closed out their session.	3.9	More Details
CVE-2024-0628	The WP RSS Aggregator plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.23.5 via the RSS feed source in admin settings. This makes it possible for authenticated attackers, with administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	3.8	More Details
CVE-2021-4437	A vulnerability, which was classified as problematic, has been found in dbartholomae lambda-middleware frameguard up to 1.0.4. Affected by this issue is some unknown functionality of the file packages/json-deserializer/src/JsonDeserializer.ts of the component JSON Mime-Type Handler. The manipulation leads to inefficient regular expression complexity. Upgrading to version 1.1.0 is able to address this issue. The patch is identified as f689404d830cbc1edd6a1018d3334ff5f44dc6a6. It is recommended to upgrade the affected component. VDB-253406 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-23319	Mattermost Jira Plugin fails to protect against logout CSRF allowing an attacker to post a specially crafted message that would disconnect a user's Jira connection in Mattermost only by viewing the message.	3.5	More Details
CVE-2024-1267	A vulnerability, which was classified as problematic, has been found in CodeAstro Restaurant POS System 1.0. Affected by this issue is some unknown functionality of the file create_account.php. The manipulation of the argument Full Name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-253010 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-24774	Mattermost Jira Plugin handling subscriptions fails to check the security level of an incoming issue or limit it based on the user who created the subscription resulting in registered users on Jira being able to create webhooks that give them access to all Jira issues.	3.4	More Details
CVE-2024-1454	The use-after-free vulnerability was found in the AuthentIC driver in OpenSC packages, occuring in the card enrolment process using pkcs15-init when a user or administrator enrols or modifies cards. An attacker must have physical access to the computer system and requires a crafted USB device or smart card to present the system with specially crafted responses to the APDUs, which are considered high complexity and low severity. This manipulation can allow for compromised card management operations during enrolment.	3.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20570	Insufficient verification of data authenticity in the configuration state machine may allow a local attacker to potentially load arbitrary bitstreams.	3.3	More Details
CVE-2024-23801	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions), Tecnomatix Plant Simulation V2302 (All versions < V2302.0007). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted SPP files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	3.3	More Details
CVE-2024-23799	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions), Tecnomatix Plant Simulation V2302 (All versions < V2302.0007). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted SPP files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	3.3	More Details
CVE-2024-22043	A vulnerability has been identified in Parasolid V35.0 (All versions < V35.0.251), Parasolid V35.1 (All versions < V35.1.170). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted XT files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	3.3	More Details
CVE-2024-23800	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions), Tecnomatix Plant Simulation V2302 (All versions < V2302.0007). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted SPP files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	3.3	More Details
CVE-2024-22226	Dell Unity, versions prior to 5.4, contain a path traversal vulnerability in its svc_supportassist utility. An authenticated attacker could potentially exploit this vulnerability, to gain unauthorized write access to the files stored on the server filesystem, with elevated privileges.	3.3	More Details
CVE-2024-24776	Mattermost fails to check the required permissions in the POST /api/v4/channels/stats/member_count API resulting in channel member counts being leaked to a user without permissions.	3.1	More Details
CVE-2024-1433	A vulnerability, which was classified as problematic, was found in KDE Plasma Workspace up to 5.93.0. This affects the function EventPluginsManager::enabledPlugins of the file components/calendar/eventpluginsmanager.cpp of the component Theme File Handler. The manipulation of the argument pluginId leads to path traversal. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The patch is named 6cdf42916369ebf4ad5bd876c4dfa0170d7b2f01. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-253407. NOTE: This requires write access to user's home or the installation of third party global themes.	3.1	More Details
CVE-2024-23760	Cleartext Storage of Sensitive Information in Gambio 4.9.2.0 allows attackers to obtain sensitive information via error-handler.log.json and legacy-error-handler.log.txt under the webroot.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1245	Concrete CMS version 9 before 9.2.5 is vulnerable to stored XSS in file tags and description attributes since administrator entered file attributes are not sufficiently sanitized in the Edit Attributes page. A rogue administrator could put malicious code into the file tags or description attributes and, when another administrator opens the same file for editing, the malicious code could execute. The Concrete CMS Security team scored this 2.4 with CVSS v3 vector AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N.	2.4	More Details
CVE-2024-1265	A vulnerability classified as problematic has been found in CodeAstro University Management System 1.0. Affected is an unknown function of the file /att_add.php of the component Attendance Management. The manipulation of the argument Student Name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-253008.	2.4	More Details
CVE-2024-1266	A vulnerability classified as problematic was found in CodeAstro University Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /st_reg.php of the component Student Registration Form. The manipulation of the argument Address 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-253009 was assigned to this vulnerability.	2.4	More Details
CVE-2024-1269	A vulnerability has been found in SourceCodester Product Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /supplier.php. The manipulation of the argument supplier_name/supplier_contact 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-253012.	2.4	More Details
CVE-2024-1247	Concrete CMS version 9 before 9.2.5 is vulnerable to stored XSS via the Role Name field since there is insufficient validation of administrator provided data for that field. A rogue administrator could inject malicious code into the Role Name field which might be executed when users visit the affected page. The Concrete CMS Security team scored this 2 with CVSS v3 vector AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator . Concrete versions below 9 do not include group types so they are not affected by this vulnerability.	2.0	More Details
CVE-2024-1246	Concrete CMS in version 9 before 9.2.5 is vulnerable to reflected XSS via the Image URL Import Feature due to insufficient validation of administrator provided data. A rogue administrator could inject malicious code when importing images, leading to the execution of the malicious code on the website user's browser. The Concrete CMS Security team scored this 2 with CVSS v3 vector AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N. This does not affect Concrete versions prior to version 9.	2.0	More Details
CVE-2023-45716	Sametime is impacted by sensitive information passed in URL.	1.7	More Details
CVE-2023-6716	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20587	Improper Access Control in System Management Mode (SMM) may allow an attacker access to the SPI flash potentially leading to arbitrary code execution.	N/A	More Details
CVE-2022-0931	Rejected reason: Red Hat Product Security does not consider this to be a vulnerability. Upstream has not acknowledged this issue as a security flaw.	N/A	More Details
CVE-2024-1420	Rejected reason: **REJECT** This is a duplicate of CVE-2024-1049. Please use CVE-2024-1049 instead.	N/A	More Details
CVE-2024-1216	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-22984	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2024-24499	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-1007. Reason: This candidate is a duplicate of CVE-2024-1007. Notes: All CVE users should reference CVE-2024-1007 instead of this candidate.	N/A	More Details
CVE-2024-24498	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-1008. Reason: This candidate is a duplicate of CVE-2024-1008. Notes: All CVE users should reference CVE-2024-1008 instead of this candidate.	N/A	More Details
CVE-2024-24497	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-1009. Reason: This candidate is a duplicate of CVE-2024-1009. Notes: All CVE users should reference CVE-2024-1009 instead of this candidate.	N/A	More Details
CVE-2024-0707	Rejected reason: **REJECT** Not a valid vulnerability.	N/A	More Details