SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 10 July 2024

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-6298	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v3.08.01; NEXUS Series v3.08.01 ; MATRIX Series v3.08.01 allows Attacker to execute arbitrary code remotely	10.0	More Details
CVE-2024-37112	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Membership Software WishList Member X.This issue affects WishList Member X: from n/a before 3.26.7.	10.0	More Details
CVE-2024-6209	Unauthorized file access in WEB Server in ABB ASPECT - Enterprise v3.08.01; NEXUS Series v3.08.01 ; MATRIX Series v3.08.01 allows Attacker to access files unauthorized	10.0	More Details
CVE-2023-38051	A BOLA vulnerability in GET, PUT, DELETE /secretaries/{secretaryId} allows a low privileged user to fetch, modify or delete a low privileged user (secretary). This results in unauthorized access and unauthorized data manipulation.	9.9	More Details
CVE-2024-37418	Unrestricted Upload of File with Dangerous Type vulnerability in Andy Moyle Church Admin allows Upload a Web Shell to a Web Server.This issue affects Church Admin: from n/a through 4.4.6.	9.9	More Details
CVE-2023-3287	A BOLA vulnerability in POST /admins allows a low privileged user to create a high privileged user (admin) in the system. This results in privilege escalation.	9.9	More Details
CVE-2023-38054	A BOLA vulnerability in GET, PUT, DELETE /customers/{customerId} allows a low privileged user to fetch, modify or delete a low privileged user (customer). This results in unauthorized access and unauthorized data manipulation.	9.9	More Details
CVE-2023-38053	A BOLA vulnerability in GET, PUT, DELETE /settings/{settingName} allows a low privileged user to fetch, modify or delete the settings of any user (including admin). This results in unauthorized access and unauthorized data manipulation.	9.9	More Details
CVE-2023-38052	A BOLA vulnerability in GET, PUT, DELETE /admins/{adminId} allows a low privileged user to fetch, modify or delete a high privileged user (admin). This results in unauthorized access and unauthorized data manipulation.	9.9	More Details
CVE-2024-3604	The OSM – OpenStreetMap plugin for WordPress is vulnerable to SQL Injection via the 'tagged_filter' attribute of the 'osm_map_v3' shortcode in all versions up to, and including, 6.0.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.9	More Details
CVE-2024-37424	Unrestricted Upload of File with Dangerous Type vulnerability in Automattic Newspack Blocks allows Upload a Web Shell to a Web Server.This issue affects Newspack Blocks: from n/a through 3.0.8.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39943	rejetto HFS (aka HTTP File Server) 3 before 0.52.10 on Linux, UNIX, and macOS allows OS command execution by remote authenticated users (if they have Upload permissions). This occurs because a shell is used to execute df (i.e., with execSync instead of spawnSync in child_process in Node.js).	9.9	More Details
CVE-2024-39932	Gogs through 0.13.0 allows argument injection during the previewing of changes.	9.9	More Details
CVE-2024-39931	Gogs through 0.13.0 allows deletion of internal files.	9.9	More Details
CVE-2024-39930	The built-in SSH server of Gogs through 0.13.0 allows argument injection in internal/ssh/ssh.go, leading to remote code execution. Authenticated attackers can exploit this by opening an SSH connection and sending a malicious --split-string env request if the built-in SSH server is activated. Windows installations are unaffected.	9.9	More Details
CVE-2023-38049	A BOLA vulnerability in GET, PUT, DELETE /appointments/{appointmentId} allows a low privileged user to fetch, modify or delete an appointment of any user (including admin). This results in unauthorized access and unauthorized data manipulation.	9.9	More Details
CVE-2023-38048	A BOLA vulnerability in GET, PUT, DELETE /providers/{providerId} allows a low privileged user to fetch, modify or delete a privileged user (provider). This results in unauthorized access and unauthorized data manipulation.	9.9	More Details
CVE-2024-37420	Unrestricted Upload of File with Dangerous Type vulnerability in WPZita Zita Elementor Site Library allows Upload a Web Shell to a Web Server.This issue affects Zita Elementor Site Library: from n/a through 1.6.1.	9.9	More Details
CVE-2024-6314	The IQ Testimonials plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the 'process_image_upload' function in versions up to, and including, 2.2.7. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. This can only be exploited if the 'gd' php extension is not loaded on the server.	9.8	More Details
CVE-2024-6602	A mismatch between allocator and deallocator could have led to memory corruption. This vulnerability affects Firefox < 128, Firefox ESR < 115.13, Thunderbird < 115.13, and Thunderbird < 128.	9.8	More Details
CVE-2024-6606	Clipboard code failed to check the index on an array access. This could have led to an out-of-bounds read. This vulnerability affects Firefox < 128 and Thunderbird < 128.	9.8	More Details
CVE-2024-6611	A nested iframe, triggering a cross-site navigation, could send SameSite=Strict or Lax cookies. This vulnerability affects Firefox < 128 and Thunderbird < 128.	9.8	More Details
CVE-2024-38074	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	9.8	More Details
CVE-2024-38076	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	9.8	More Details
CVE-2024-38077	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	9.8	More Details
CVE-2024-39171	Directory Travel in PHPVibe v11.0.46 due to incomplete blacklist checksums and directory checks, which can lead to code execution via writing specific statements to .htaccess and code to a file with a .png suffix.	9.8	More Details
CVE-2023-48194	Vulnerability in Tenda AC8v4 .V16.03.34.09 due to sscanf and the last digit of s8 being overwritten with \x0. After executing set_client_qos, control over the gp register can be obtained.	9.8	More Details
CVE-2024-37870	SQL injection vulnerability in processscore.php in Learning Management System Project In PHP With Source Code 1.0 allows attackers to execute arbitrary SQL commands via the id parameter.	9.8	More Details
CVE-2024-37873	SQL injection vulnerability in view_payslip.php in Itsourcecode Payroll Management System Project In PHP With Source Code 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	9.8	More Details
CVE-2024-36526	ZKTeco ZKBio CVSecurity v6.1.1 was discovered to contain a hardcoded cryptographic key.	9.8	More Details
CVE-2024-39071	Fujian Kelixun <=7.6.6.4391 is vulnerable to SQL Injection in send_event.php.	9.8	More Details
CVE-2024-39223	An authentication bypass in the SSH service of gost v2.11.5 allows attackers to intercept communications via setting the HostKeyCallback function to ssh.InsecureIgnoreHostKey	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39028	An issue was discovered in SeaCMS <=12.9 which allows remote attackers to execute arbitrary code via admin_ping.php.	9.8	More Details
CVE-2024-27709	SQL Injection vulnerability in Eskooly Web Product v.3.0 allows a remote attacker to execute arbitrary code via the searchby parameter of the allstudents.php component and the id parameter of the requestmanager.php component.	9.8	More Details
CVE-2024-27710	An issue in Eskooly Free Online School management Software v.3.0 and before allows a remote attacker to escalate privileges via the authentication mechanism.	9.8	More Details
CVE-2024-39864	The CloudStack integration API service allows running its unauthenticated API server (usually on port 8096 when configured and enabled via integration.api.port global setting) for internal portal integrations and for testing purposes. By default, the integration API service port is disabled and is considered disabled when integration.api.port is set to 0 or negative. Due to an improper initialisation logic, the integration API service would listen on a random port when its port value is set to 0 (default value). An attacker that can access the CloudStack management network could scan and find the randomised integration API service port and exploit it to perform unauthorised administrative actions and perform remote code execution on CloudStack managed hosts and result in complete compromise of the confidentiality, integrity, and availability of CloudStack managed infrastructure. Users are recommended to restrict the network access on the CloudStack management server hosts to only essential ports. Users are recommended to upgrade to version 4.18.2.1, 4.19.0.2 or later, which addresses this issue.	9.8	More Details
CVE-2024-6313	The Gutenberg Forms plugin for WordPress is vulnerable to arbitrary file uploads due to the users can specify the allowed file types in the 'upload' function in versions up to, and including, 2.2.9. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2024-27712	An issue in Eskooly Free Online School management Software v.3.0 and before allows a remote attacker to escalate privileges via the User Account Mangemnt component in the authentication mechanism.	9.8	More Details
CVE-2024-40614	EGroupware before 23.1.20240624 mishandles an ORDER BY clause. This leads to json.php?menuaction=EGroupware\Api\Etemplate\Widget\Nextmatch::ajax_get_rows sort.id SQL injection by authenticated users for Address Book or InfoLog sorting.	9.8	More Details
CVE-2024-27903	OpenVPN plug-ins on Windows with OpenVPN 2.6.9 and earlier could be loaded from any directory, which allows an attacker to load an arbitrary plug-in which can be used to interact with the privileged OpenVPN interactive service.	9.8	More Details
CVE-2023-46685	A hard-coded password vulnerability exists in the telnetd functionality of LevelOne WBR-6013 RER4_A_v3411b_2T2R_LEV_09_170623. A set of specially crafted network packets can lead to arbitrary command execution.	9.8	More Details
CVE-2024-1305	tap-windows6 driver version 9.26 and earlier does not properly check the size data of incomming write operations which an attacker can use to overflow memory buffers, resulting in a bug check and potentially arbitrary code execution in kernel space	9.8	More Details
CVE-2024-6365	The Product Table by WBW plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.0.1 via the 'saveCustomTitle' function. This is due to missing authorization and lack of sanitization of appended data in the languages/customTitle.php file. This makes it possible for unauthenticated attackers to execute code on the server.	9.8	More Details
CVE-2024-5488	The SEOPress WordPress plugin before 7.9 does not properly protect some of its REST API routes, which combined with another Object Injection vulnerability can allow unauthenticated attackers to unserialize malicious gadget chains, compromising the site if a suitable chain is present.	9.8	More Details
CVE-2024-28747	An unauthenticated remote attacker can use the hard-coded credentials to access the SmartSPS devices with high privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38346	The CloudStack cluster service runs on unauthenticated port (default 9090) that can be misused to run arbitrary commands on targeted hypervisors and CloudStack management server hosts. Some of these commands were found to have command injection vulnerabilities that can result in arbitrary code execution via agents on the hosts that may run as a privileged user. An attacker that can reach the cluster service on the unauthenticated port (default 9090), can exploit this to perform remote code execution on CloudStack managed hosts and result in complete compromise of the confidentiality, integrity, and availability of CloudStack managed infrastructure. Users are recommended to restrict the network access to the cluster service port (default 9090) on a CloudStack management server host to only its peer CloudStack management server hosts. Users are recommended to upgrade to version 4.18.2.1, 4.19.0.2 or later, which addresses this issue.	9.8	More Details
CVE-2024-39165	QR/demoapp/qr_image.php in Asial JpGraph Professional through 4.2.6-pro allows remote attackers to execute arbitrary code via a PHP payload in the data parameter in conjunction with a .php file name in the filename parameter. This occurs because an unnecessary QR/demoapp folder.is shipped with the product.	9.8	More Details
CVE-2024-39844	In ZNC before 1.9.1, remote code execution can occur in modtcl via a KICK.	9.8	More Details
CVE-2024-29319	Volmarg Personal Management System 1.4.64 is vulnerable to SSRF (Server Side Request Forgery) via uploading a SVG file. The server can make unintended HTTP and DNS requests to a server that the attacker controls.	9.8	More Details
CVE-2024-23998	goanother Another Redis Desktop Manager =<1.6.1 is vulnerable to Cross Site Scripting (XSS) via src/components/Setting.vue.	9.6	More Details
CVE-2024-23997	Lukas Bach yana =<1.0.16 is vulnerable to Cross Site Scripting (XSS) via src/electron-main.ts.	9.6	More Details
CVE-2024-39872	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application does not properly assign rights to temporary files created during its update process. This could allow an authenticated attacker with the 'Manage firmware updates' role to escalate their privileges on the underlying OS level.	9.6	More Details
CVE-2023-38055	A BOLA vulnerability in GET, PUT, DELETE /services/{serviceId} allows a low privileged user to fetch, modify or delete the services of any user (including admin). This results in unauthorized access and unauthorized data manipulation.	9.6	More Details
CVE-2024-37768	14Finger v1.1 was discovered to contain an arbitrary user deletion vulnerability via the component /api/admin/user?id.	9.1	More Details
CVE-2024-38089	Microsoft Defender for IoT Elevation of Privilege Vulnerability	9.1	More Details
CVE-2023-38050	A BOLA vulnerability in GET, PUT, DELETE /webhooks/{webhookId} allows a low privileged user to fetch, modify or delete a webhook of any user (including admin). This results in unauthorized access and unauthorized data manipulation.	9.1	More Details
CVE-2024-28751	An high privileged remote attacker can enable telnet access that accepts hardcoded credentials.	9.1	More Details
CVE-2024-37555	Unrestricted Upload of File with Dangerous Type vulnerability in ZealousWeb Generate PDF using Contact Form 7.This issue affects Generate PDF using Contact Form 7: from n/a through 4.0.6.	9.1	More Details
CVE-2024-37082	When deploying Cloud Foundry together with the haproxy-boshrelease and using a non default configuration, it might be possible to craft HTTP requests that bypass mTLS authentication to Cloud Foundry applications. You are affected if you have route-services enabled in routing-release and have configured the haproxy-boshrelease property “ha_proxy.forwarded_client_cert” to “forward_only_if_route_service”.	9.1	More Details
CVE-2024-3596	RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2024-21428	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-5943	The Nested Pages plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.2.7. This is due to missing or incorrect nonce validation on the 'settingsPage' function and missing santization of the 'tab' parameter. This makes it possible for unauthenticated attackers to call local php files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2024-21449	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-39202	D-Link DIR-823X firmware - 240126 was discovered to contain a remote command execution (RCE) vulnerability via the dhcpd_startip parameter at /goform/set_lan_settings.	8.8	More Details
CVE-2024-39935	jc21 NGINX Proxy Manager before 2.11.3 allows backend/internal/certificate.js OS command injection by an authenticated user (with certificate management privileges) via untrusted input to the DNS provider configuration. NOTE: this is not part of any NGINX software shipped by F5.	8.8	More Details
CVE-2024-39063	Lime Survey <= 6.5.12 is vulnerable to Cross Site Request Forgery (CSRF). The YII_CSRF_TOKEN is only checked when passed in the body of POST requests, but the same check isn't performed in the equivalent GET requests.	8.8	More Details
CVE-2024-35256	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-38104	Windows Fax Service Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-5793	The Houzez Theme - Functionality plugin for WordPress is vulnerable to SQL Injection via the ‘currency_code’ parameter in all versions up to, and including, 3.2.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Custom-level (seller) 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-2024-38092	Azure CycleCloud Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-38088	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-38087	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-6166	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to time-based SQL Injection via the ‘addons_order’ parameter in all versions up to, and including, 1.5.112 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 and granted plugin setting edit permissions by an administrator, 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-2024-5441	The Modern Events Calendar plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the set_featured_image function in all versions up to, and including, 7.11.0. This makes it possible for authenticated attackers, with subscriber access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. The plugin allows administrators (via its settings) to extend the ability to submit events to unauthenticated users, which would allow unauthenticated attackers to exploit this vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30013	Windows MultiPoint Services Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-39881	Delta Electronics CNCSoft-G2 lacks proper validation of user-supplied data, which can result in a memory corruption condition. If a target visits a malicious page or opens a malicious file an attacker can leverage this vulnerability to execute code in the context of the current process.	8.8	More Details
CVE-2024-6161	The Default Thumbnail Plus plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'get_cache_image' function in all versions up to, and including, 1.0.2.3. This makes it possible for authenticated attackers, with contributor-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2024-6319	The IMGspider plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload' function in all versions up to, and including, 2.3.10. This makes it possible for authenticated attackers, with contributor-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2024-6318	The IMGspider plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload_img_file' function in all versions up to, and including, 2.3.10. This makes it possible for authenticated attackers, with contributor-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2024-3904	Incorrect Default Permissions vulnerability in Smart Device Communication Gateway preinstalled on MELIPC Series MI5122-VW firmware versions "05" to "07" allows a local attacker to execute arbitrary code by saving a malicious file to a specific folder. As a result, the attacker may disclose, tamper with, destroy or delete information in the product, or cause a denial-of-service (DoS) condition on the product.	8.8	More Details
CVE-2024-6309	The Attachment File Icons (AF Icons) plugin for WordPress is vulnerable to Cross-Site Request Forgery to Arbitrary File Upload in versions up to, and including, 1.3. This is due to missing nonce validation in the 'afi_overview' function and missing file type validation in the 'upload_icons' function. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2024-39696	Evmos is a decentralized Ethereum Virtual Machine chain on the Cosmos Network. Prior to version 19.0.0, a user can create a vesting account with a 3rd party account (EOA or contract) as funder. Then, this user can create an authorization for the contract.CallerAddress, this is the authorization checked in the code. But the funds are taken from the funder address provided in the message. Consequently, the user can fund a vesting account with a 3rd party account without its permission. The funder address can be any address, so this vulnerability can be used to drain all the accounts in the chain. The issue has been patched in version 19.0.0.	8.8	More Details
CVE-2024-6316	The Generate PDF using Contact Form 7 plugin for WordPress is vulnerable to Cross-Site Request Forgery to Arbitrary File Upload in versions up to, and including, 4.0.6. This is due to missing nonce validation and missing file type validation in the 'wp_cf7_pdf_dashboard_html_page' function. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2024-6317	The Generate PDF using Contact Form 7 plugin for WordPress is vulnerable to Cross-Site Request Forgery to Arbitrary File Upload in versions up to, and including, 4.0.6. This is due to missing nonce validation and the plugin not properly validating a file or its path prior to deleting it in the 'wp_cf7_pdf_dashboard_html_page' function. This makes it possible for unauthenticated attackers to delete arbitrary files, including the wp-config.php file, which can make site takeover and remote code execution possible via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2024-6320	The ScrollTo Top plugin for WordPress is vulnerable to Cross-Site Request Forgery to Arbitrary File Upload in versions up to, and including, 1.2.2. This is due to missing nonce validation and missing file type validation in the 'options_page' function. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2024-6321	The ScrollTo Bottom plugin for WordPress is vulnerable to Cross-Site Request Forgery to Arbitrary File Upload in versions up to, and including, 1.1.1. This is due to missing nonce validation and missing file type validation in the 'options_page' function. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2385	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 8.3.7 via several of the plugin's widgets through the 'style' attribute. This makes it possible for authenticated attackers, with contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	8.8	More Details
CVE-2024-5456	The Panda Video plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.4.0 via the 'selected_button' parameter. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	8.8	More Details
CVE-2023-47677	A cross-site request forgery (csrf) vulnerability exists in the boa CSRF protection functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted network request can lead to CSRF. An attacker can send an HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2024-35271	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-35272	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37318	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-39022	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/infoSys_deal.php?mudi=deal	8.8	More Details
CVE-2024-37336	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37334	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37333	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37332	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37331	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37330	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-27713	An issue in Eskooly Free Online School management Software v.3.0 and before allows a remote attacker to escalate privileges via the HTTP Response Header Settings component.	8.8	More Details
CVE-2024-27711	An issue in Eskooly Free Online School management Software v.3.0 and before allows a remote attacker to escalate privileges via the Sin-up process function in the account settings.	8.8	More Details
CVE-2024-37329	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37769	Insecure permissions in 14Finger v1.1 allow attackers to escalate privileges from normal user to Administrator via a crafted POST request.	8.8	More Details
CVE-2024-37328	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37327	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37326	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37324	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-40034	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/userLevel_deal.php?mudi=del	8.8	More Details
CVE-2024-37973	Secure Boot Security Feature Bypass Vulnerability	8.8	More Details
CVE-2024-40036	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/userGroup_deal.php?mudi=add&nohrefStr=close	8.8	More Details
CVE-2024-40037	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/userScore_deal.php?mudi=del	8.8	More Details
CVE-2024-40039	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/userGroup_deal.php?mudi=del	8.8	More Details
CVE-2024-37323	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37322	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37321	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37320	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-37319	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-38060	Windows Imaging Component Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6310	The Advanced AJAX Page Loader plugin for WordPress is vulnerable to Cross-Site Request Forgery to Arbitrary File Upload in versions up to, and including, 2.7.7. This is due to missing nonce validation in the 'admin_init_AAPL' function and missing file type validation in the 'AAPL_options_validate' function. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2024-6069	The Registration Forms – User Registration Forms, Invitation-Based Registrations, Front-end User Profile, Login Form & Content Restriction plugin for WordPress is vulnerable to unauthorized arbitrary plugin installation and activation/deactivation due to missing capability checks on the pieregister_install_addon, pieregister_activate_addon and pieregister_deactivate_addon functions in all versions up to, and including, 3.8.3.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install, activate and deactivate arbitrary plugins. As a result attackers might achieve code execution on the targeted server	8.8	More Details
CVE-2024-29509	Artifex Ghostscript before 10.03.0 has a heap-based overflow when PDFPassword (e.g., for runpdf) has a \000 byte in the middle.	8.8	More Details
CVE-2024-29506	Artifex Ghostscript before 10.03.0 has a stack-based buffer overflow in the pdfi_apply_filter() function via a long PDF filter name.	8.8	More Details
CVE-2024-39866	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application allows users to upload encrypted backup files. This could allow an attacker with access to the backup encryption key and with the right to upload backup files to create a user with administrative privileges.	8.8	More Details
CVE-2024-39882	Delta Electronics CNCSoft-G2 lacks proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. If a target visits a malicious page or opens a malicious file an attacker can leverage this vulnerability to execute code in the context of the current process.	8.8	More Details
CVE-2024-37952	Improper Privilege Management vulnerability in themeenergy BookYourTravel allows Privilege Escalation.This issue affects BookYourTravel: from n/a through 8.18.17.	8.8	More Details
CVE-2024-6605	Firefox Android allowed immediate interaction with permission prompts. This could be used for tapjacking. This vulnerability affects Firefox < 128.	8.8	More Details
CVE-2024-6607	It was possible to prevent a user from exiting pointerlock when pressing escape and to overlay customValidity notifications from a `<select>` element over certain permission prompts. This could be used to confuse a user into giving a site unintended permissions. This vulnerability affects Firefox < 128 and Thunderbird < 128.	8.8	More Details
CVE-2024-6609	When almost out-of-memory an elliptic curve key which was never allocated could have been freed again. This vulnerability affects Firefox < 128 and Thunderbird < 128.	8.8	More Details
CVE-2024-6615	Memory safety bugs present in Firefox 127 and Thunderbird 127. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 128 and Thunderbird < 128.	8.8	More Details
CVE-2024-38021	Microsoft Outlook Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-23663	An improper access control in Fortinet FortiExtender 4.1.1 - 4.1.9, 4.2.0 - 4.2.6, 5.3.2, 7.0.0 - 7.0.4, 7.2.0 - 7.2.4 and 7.4.0 - 7.4.2 allows an attacker to create users with elevated privileges via a crafted HTTP request.	8.8	More Details
CVE-2024-27784	Multiple Exposure of sensitive information to an unauthorized actor vulnerabilities [CWE-200] in FortiAIOps version 2.0.0 may allow an authenticated, remote attacker to retrieve sensitive information from the API endpoint or log files.	8.8	More Details
CVE-2024-20701	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21303	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21308	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21317	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21331	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21332	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-2376	The WPQA Builder WordPress plugin before 6.1.1 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	8.8	More Details
CVE-2024-21333	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21335	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21373	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21398	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21414	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21415	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-21425	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-39865	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application allows users to upload encrypted backup files. As part of this backup, files can be restored without correctly checking the path of the restored file. This could allow an attacker with access to the backup encryption key to upload malicious files, that could potentially lead to remote code execution.	8.8	More Details
CVE-2024-39023	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via admin/info_deal.php?mudi=add&nohrefStr=close	8.8	More Details
CVE-2024-28928	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39571	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 HF1). Affected applications are vulnerable to command injection due to missing server side input sanitation when loading SNMP configurations. This could allow an attacker with the right to modify the SNMP configuration to execute arbitrary code with root privileges.	8.8	More Details
CVE-2024-38053	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2024-33871	An issue was discovered in Artifex Ghostscript before 10.03.1. contrib/opvp/gdevopvp.c allows arbitrary code execution via a custom Driver library, exploitable via a crafted PostScript document. This occurs because the Driver parameter for opvp (and oprp) devices can have an arbitrary name for a dynamic library; this library is then loaded.	8.8	More Details
CVE-2024-34722	In smp_proc_rand of smp_act.cc, there is a possible authentication bypass during legacy BLE pairing due to incorrect implementation of a protocol. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2024-37455	Improper Privilege Management vulnerability in Brainstorm Force Ultimate Addons for Elementor allows Privilege Escalation.This issue affects Ultimate Addons for Elementor: from n/a through 1.36.31.	8.8	More Details
CVE-2024-37829	An issue in Outline <= v0.76.1 allows attackers to execute a session hijacking attack via user interaction with a crafted magic sign-in link.	8.8	More Details
CVE-2024-37484	Improper Privilege Management vulnerability in Dylan James Zephyr Project Manager allows Privilege Escalation.This issue affects Zephyr Project Manager: from n/a through 3.3.97.	8.8	More Details
CVE-2024-39883	Delta Electronics CNCSoft-G2 lacks proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. If a target visits a malicious page or opens a malicious file an attacker can leverage this vulnerability to execute code in the context of the current process.	8.8	More Details
CVE-2024-39570	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 HF1). Affected applications are vulnerable to command injection due to missing server side input sanitation when loading VxLAN configurations. This could allow an authenticated attacker to execute arbitrary code with root privileges.	8.8	More Details
CVE-2024-28899	Secure Boot Security Feature Bypass Vulnerability	8.8	More Details
CVE-2024-39675	A vulnerability has been identified in RUGGEDCOM RMC30 (All versions < V4.3.10), RUGGEDCOM RMC30NC (All versions < V4.3.10), RUGGEDCOM RP110 (All versions < V4.3.10), RUGGEDCOM RP110NC (All versions < V4.3.10), RUGGEDCOM RS400 (All versions < V4.3.10), RUGGEDCOM RS400NC (All versions < V4.3.10), RUGGEDCOM RS401 (All versions < V4.3.10), RUGGEDCOM RS401NC (All versions < V4.3.10), RUGGEDCOM RS416 (All versions < V4.3.10), RUGGEDCOM RS416NC (All versions < V4.3.10), RUGGEDCOM RS416NCv2 V4.X (All versions < V4.3.10), RUGGEDCOM RS416NCv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416P (All versions < V4.3.10), RUGGEDCOM RS416PNC (All versions < V4.3.10), RUGGEDCOM RS416PNCv2 V4.X (All versions < V4.3.10), RUGGEDCOM RS416PNCv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416Pv2 V4.X (All versions < V4.3.10), RUGGEDCOM RS416Pv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416v2 V4.X (All versions < V4.3.10), RUGGEDCOM RS416v2 V5.X (All versions < V5.9.0), RUGGEDCOM RS910 (All versions < V4.3.10), RUGGEDCOM RS910L (All versions), RUGGEDCOM RS910LNC (All versions), RUGGEDCOM RS910NC (All versions < V4.3.10), RUGGEDCOM RS910W (All versions < V4.3.10), RUGGEDCOM RS920L (All versions), RUGGEDCOM RS920LNC (All versions), RUGGEDCOM RS920W (All versions). In some configurations the affected products wrongly enable the Modbus service in non-managed VLANS. Only serial devices are affected by this vulnerability.	8.8	More Details
CVE-2024-39936	An issue was discovered in HTTP2 in Qt before 5.15.18, 6.x before 6.2.13, 6.3.x through 6.5.x before 6.5.7, and 6.6.x through 6.7.x before 6.7.3. Code to make security-relevant decisions about an established connection may execute too early, because the encrypted() signal has not yet been emitted and processed..	8.6	More Details
CVE-2024-39697	phonenumber is a library for parsing, formatting and validating international phone numbers. Since 0.3.4, the phonenumber parsing code may panic due to a panic-guarded out-of-bounds access on the phonenumber string. In a typical deployment of rust-phonenumber, this may get triggered by feeding a maliciously crafted phonenumber, e.g. over the network, specifically strings of the form `+dwPAA;phone-context=AA`, where the "number" part potentially parses as a number larger than 2^56. This vulnerability is fixed in 0.3.6.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39937	supOS 5.0 allows api/image/download?fileName=../ directory traversal for reading files.	8.6	More Details
CVE-2024-37494	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in KaineLabs Youzify.This issue affects Youzify: from n/a through 1.2.5.	8.5	More Details
CVE-2024-34361	Pi-hole is a DNS sinkhole that protects devices from unwanted content without installing any client-side software. A vulnerability in versions prior to 5.18.3 allows an authenticated user to make internal requests to the server via the `gravity_DownloadBlocklistFromUrl()` function. Depending on some circumstances, the vulnerability could lead to remote command execution. Version 5.18.3 contains a patch for this issue.	8.5	More Details
CVE-2024-37513	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Themewinter WPCafe allows Path Traversal.This issue affects WPCafe: from n/a through 2.2.27.	8.5	More Details
CVE-2024-38363	Airbyte is a data integration platform for ELT pipelines. Airbyte connection builder docker image is vulnerable to RCE via SSTI which allows an authenticated remote attacker to execute arbitrary code on the server as the web server user. The connection builder is used to create and test new connectors. Sensitive information, such as credentials, could be exposed if a user tested a new connector on a compromised instance. The connection builder does not have access to any data processes. This vulnerability is fixed in 0.62.2.	8.5	More Details
CVE-2024-37501	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in PluginsWare Advanced Classifieds & Directory Pro allows Path Traversal.This issue affects Advanced Classifieds & Directory Pro: from n/a through 3.1.3.	8.5	More Details
CVE-2024-37090	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in StylemixThemes Masterstudy Elementor Widgets, StylemixThemes Consulting Elementor Widgets.This issue affects Masterstudy Elementor Widgets: from n/a through 1.2.2; Consulting Elementor Widgets: from n/a through 1.3.0.	8.5	More Details
CVE-2023-3288	A BOLA vulnerability in POST /providers allows a low privileged user to create a privileged user (provider) in the system. This results in privilege escalation.	8.5	More Details
CVE-2024-37268	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in kaptinlin Striking allows Path Traversal.This issue affects Striking: from n/a through 2.3.4.	8.5	More Details
CVE-2023-38047	A BOLA vulnerability in GET, PUT, DELETE /categories/{categoryId} allows a low privileged user to fetch, modify or delete the category of any user (including admin). This results in unauthorized access and unauthorized data manipulation.	8.5	More Details
CVE-2024-37225	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Zoho Marketing Automation.This issue affects Zoho Marketing Automation: from n/a through 1.2.7.	8.5	More Details
CVE-2024-37462	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in G5Theme Ultimate Bootstrap Elements for Elementor allows Path Traversal.This issue affects Ultimate Bootstrap Elements for Elementor: from n/a through 1.4.2.	8.5	More Details
CVE-2023-52168	The NtfsHandler.cpp NTFS handler in 7-Zip before 24.01 (for 7zz) contains a heap-based buffer overflow that allows an attacker to overwrite two bytes at multiple offsets beyond the allocated buffer size: buffer+512*i-2, for i=9, i=10, i=11, etc.	8.4	More Details
CVE-2023-50806	A vulnerability was discovered in Samsung Mobile Processor, Wearable Processor, and Modems with versions Exynos 9820, Exynos 9825, Exynos 980, Exynos 990, Exynos 850 Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380 Exynos 1330, Exynos 9110, Exynos W920, Exynos W930, Exynos Modem 5123, Exynos Modem 5300 that allows out-of-bounds access to a heap buffer in the SIM Proactive Command.	8.4	More Details
CVE-2024-37984	Secure Boot Security Feature Bypass Vulnerability	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27715	An issue in Eskooly Free Online School management Software v.3.0 and before allows a remote attacker to escalate privileges via a crafted request to the Password Change mechanism.	8.2	More Details
CVE-2023-52169	The NtfsHandler.cpp NTFS handler in 7-Zip before 24.01 (for 7zz) contains an out-of-bounds read that allows an attacker to read beyond the intended buffer. The bytes read beyond the intended buffer are presented as a part of a filename listed in the file system image. This has security relevance in some known web-service use cases where untrusted users can upload files and have them extracted by a server-side 7-Zip process.	8.2	More Details
CVE-2024-37871	SQL injection vulnerability in login.php in Itsourcecode Online Discussion Forum Project in PHP with Source Code 1.0 allows remote attackers to execute arbitrary SQL commands via the email parameter.	8.2	More Details
CVE-2024-37903	Mastodon is a self-hosted, federated microblogging platform. Starting in version 2.6.0 and prior to versions 4.1.18 and 4.2.10, by crafting specific activities, an attacker can extend the audience of a post they do not own to other Mastodon users on a target server, thus gaining access to the contents of a post not intended for them. Versions 4.1.18 and 4.2.10 contain a patch for this issue.	8.2	More Details
CVE-2024-22271	In Spring Cloud Function framework, versions 4.1.x prior to 4.1.2, 4.0.x prior to 4.0.8 an application is vulnerable to a DOS attack when attempting to compose functions with non-existing functions. Specifically, an application is vulnerable when all of the following are true: User is using Spring Cloud Function Web module Affected Spring Products and Versions Spring Cloud Function Framework 4.1.0 to 4.1.2 4.0.0 to 4.0.8 References https://spring.io/security/cve-2022-22979 https://checkmarx.com/blog/spring-function-cloud-dos-cve-2022-22979-and-unintended-function-invocation/ History 2020-01-16: Initial vulnerability report published.	8.2	More Details
CVE-2024-6506	Information exposure vulnerability in the MRW plugin, in its 5.4.3 version, affecting the "mrw_log" functionality. This vulnerability could allow a remote attacker to obtain other customers' order information and access sensitive information such as name and phone number. This vulnerability also allows an attacker to create or overwrite shipping labels.	8.2	More Details
CVE-2023-50807	A vulnerability was discovered in Samsung Wearable Processor and Modems with versions Exynos 9110, Exynos Modem 5123, Exynos Modem 5300 that allows an out-of-bounds write in the heap in 2G (no auth).	8.1	More Details
CVE-2024-38345	A cross-site request forgery vulnerability exists in Sola Testimonials versions prior to 3.0.0. If this vulnerability is exploited, an attacker allows a user who logs in to the WordPress site where the affected plugin is enabled to access a malicious page. As a result, the user may perform unintended operations on the WordPress site.	8.1	More Details
CVE-2023-50805	A vulnerability was discovered in Samsung Mobile Processor, Wearable Processor, and Modems with versions Exynos 9820, Exynos 9825, Exynos 980, Exynos 990, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 9110, Exynos W920, Exynos W930, Exynos Modem 5123, Exynos Modem 5300 that allows an out-of-bounds write in the heap in 2G (no auth).	8.1	More Details
CVE-2024-39830	Mattermost versions 9.8.x <= 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2 and 9.5.x <= 9.5.5, when shared channels are enabled, fail to use constant time comparison for remote cluster tokens which allows an attacker to retrieve the remote cluster token via a timing attack during remote cluster token comparison.	8.1	More Details
CVE-2024-27782	Multiple insufficient session expiration vulnerabilities [CWE-613] in FortiAIOps version 2.0.0 may allow an attacker to re-use stolen old session tokens to perform unauthorized operations via crafted requests.	8.1	More Details
CVE-2024-6426	Information exposure vulnerability in MESbook 20221021.03 version, the exploitation of which could allow a local attacker, with user privileges, to access different resources by changing the API value of the application.	8.1	More Details
CVE-2024-6507	Command injection when ingesting a remote Kaggle dataset due to a lack of input sanitization in the ingest_kaggle() API	8.1	More Details
CVE-2024-32937	An os command injection vulnerability exists in the CWMP SelfDefinedTimeZone functionality of Grandstream GXP2135 1.0.9.129, 1.0.11.74 and 1.0.11.79. A specially crafted network packet can lead to arbitrary command execution. An attacker can send a sequence of malicious packets to trigger this vulnerability.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29153	A vulnerability was discovered in Samsung Mobile Processor, Wearable Processor, and Modems with versions Exynos 9820, Exynos 9825, Exynos 980, Exynos 990, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 9110, Exynos W920, Exynos W930, Exynos Modem 5123, and Exynos Modem 5300 that involves incorrect authorization of LTE NAS messages and leads to downgrading to lower network generations and repeated DDOS.	8.1	More Details
CVE-2024-39742	IBM MQ Operator 3.2.2 and IBM MQ Operator 2.0.24 could allow a user to bypass authentication under certain configurations due to a partial string comparison vulnerability. IBM X-Force ID: 297169.	8.1	More Details
CVE-2024-37872	SQL injection vulnerability in process.php in Itsourcecode Billing System in PHP 1.0 allows remote attackers to execute arbitrary SQL commands via the username parameter.	8.1	More Details
CVE-2024-35264	.NET and Visual Studio Remote Code Execution Vulnerability	8.1	More Details
CVE-2024-38011	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-37969	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-38010	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-37970	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-37989	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-37988	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-37981	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-37986	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-37977	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-37975	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-37978	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-37971	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37987	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-37972	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-37974	Secure Boot Security Feature Bypass Vulnerability	8.0	More Details
CVE-2024-38043	PowerShell Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38050	Windows Workstation Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-45147	A vulnerability has been identified in SIMATIC PCS neo V4.0 (All versions), SIMATIC STEP 7 V16 (All versions), SIMATIC STEP 7 V17 (All versions), SIMATIC STEP 7 V18 (All versions < V18 Update 2). Affected applications do not properly restrict the .NET BinaryFormatter when deserializing user-controllable input. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application. This is the same issue that exists for .NET BinaryFormatter https://docs.microsoft.com/en-us/visualstudio/code-quality/ca2300.	7.8	More Details
CVE-2024-38047	PowerShell Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-32056	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted IGS part file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-33653	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted BMP files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-33654	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted BMP files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-37997	A vulnerability has been identified in JT Open (All versions < V11.5), JT2Go (All versions < V2406.0003), PLM XML SDK (All versions < V7.1.0.014), Teamcenter Visualization V14.2 (All versions < V14.2.0.13), Teamcenter Visualization V14.3 (All versions < V14.3.0.11), Teamcenter Visualization V2312 (All versions < V2312.0008), Teamcenter Visualization V2406 (All versions < V2406.0003). The affected applications contain a stack based overflow vulnerability while parsing specially crafted XML files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2024-31313	In availableToWriteBytes of MessageQueueBase.h, there is a possible out of bounds write due to an incorrect 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-2024-38052	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38080	Windows Hyper-V Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-39567	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 HF1). The system service of affected applications is vulnerable to command injection due to missing server side input sanitation when loading VPN configurations. This could allow an authenticated local attacker to execute arbitrary code with system privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39568	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 HF1). The system service of affected applications is vulnerable to command injection due to missing server side input sanitation when loading proxy configurations. This could allow an authenticated local attacker to execute arbitrary code with system privileges.	7.8	More Details
CVE-2024-31315	In multiple functions of ManagedServices.java, there is a possible way to hide an app with notification access in the Device & app notifications settings due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2024-31316	In onResult of AccountManagerService.java, there is a possible way to perform an arbitrary background activity launch due to parcel mismatch. 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-2024-38051	Windows Graphics Component Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-31311	In increment_annotation_count of stats_event.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-39934	Robotmk before 2.0.1 allows a local user to escalate privileges (e.g., to SYSTEM) if automated Python environment setup is enabled, because the "shared holotree usage" feature allows any user to edit any Python environment.	7.8	More Details
CVE-2024-36041	KSmserver in KDE Plasma Workspace (aka plasma-workspace) before 5.27.11.1 and 6.x before 6.0.5.1 allows connections via ICE based purely on the host, i.e., all local connections are accepted. This allows another user on the same machine to gain access to the session manager, e.g., use the session-restore feature to execute arbitrary code as the victim (on the next boot) via earlier use of the /tmp directory.	7.8	More Details
CVE-2024-38085	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21113	In multiple locations, there is a possible permission bypass due to a confused deputy. 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-2024-39880	Delta Electronics CNCSoft-G2 lacks proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. If a target visits a malicious page or opens a malicious file an attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2023-21114	In multiple locations, there is a possible permission bypass due to a confused deputy. 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-2024-23695	In CacheOpPMRExec of cache_km.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-30079	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38070	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability	7.8	More Details
CVE-2024-23696	In RGXCreateZSBufferKM of rgxta3d.c, there is a possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-4944	A local privilege escalation vlnerability in the WatchGuard Mobile VPN with SSL client on Windows enables a local user to execute arbitrary commands with elevated privileged.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38100	Windows File Explorer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38066	Windows Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38062	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-23697	In RGXCreateHWRTData_aux of rgxta3d.c, there is a possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-38059	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-23698	In RGXFWChangeOSidPriority of rgxfwutils.c, there is a possible arbitrary code execution due to a missing bounds check. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-38057	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-23711	In DevmemXIntUnreserveRange of devicemem_server.c, there is a possible arbitrary code execution due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-38054	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-31310	In newServiceInfoLocked of AutofillManagerServiceImpl.java, there is a possible way to hide an enabled Autofill service app in the Autofill service settings due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2024-35261	Azure Network Watcher VM Extension Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-38079	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-31332	In multiple locations, there is a possible way to bypass a restriction on adding new Wi-Fi connections due to a missing permission 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-2024-31334	In DevmemIntFreeDefBackingPage of devicemem_server.c, there is a possible arbitrary code execution due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-31322	In updateServicesLocked of AccessibilityManagerService.java, there is a possible way for an app to be hidden from the Setting while retaining Accessibility Service due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2024-34726	In PVRSRV_MMap of pvr_bridge_k.c, there is a possible arbitrary code execution due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-31317	In multiple functions of ZygoteProcess.java, there is a possible way to achieve code execution as any app via WRITE_SECURE_SETTINGS due to unsafe deserialization. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31323	In onCreate of multiple files, there is a possible way to trick the user into granting health permissions due to tapjacking. 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-2024-38517	Tencent RapidJSON is vulnerable to privilege escalation due to an integer underflow in the `GenericReader::ParseNumber()` function of `include/rapidjson/reader.h` when parsing JSON text from a stream. An attacker needs to send the victim a crafted file which needs to be opened; this triggers the integer underflow vulnerability (when the file is parsed), leading to elevation of privilege.	7.8	More Details
CVE-2024-31319	In updateNotificationChannelFromPrivilegedListener of NotificationManagerService.java, there is a possible cross-user data leak due to a confused deputy. 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-2024-39684	Tencent RapidJSON is vulnerable to privilege escalation due to an integer overflow in the `GenericReader::ParseNumber()` function of `include/rapidjson/reader.h` when parsing JSON text from a stream. An attacker needs to send the victim a crafted file which needs to be opened; this triggers the integer overflow vulnerability (when the file is parsed), leading to elevation of privilege.	7.8	More Details
CVE-2024-31318	In CompanionDeviceManagerService.java, there is a possible way to pair a companion device without user acceptance due to a missing permission 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-2024-31325	In multiple locations, there is a possible way to reveal images across users data due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-31326	In multiple locations, there is a possible way in which policy migration code will never be executed due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-20781	InDesign Desktop versions ID19.3, ID18.5.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-20782	InDesign Desktop versions ID19.3, ID18.5.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-34723	In onTransact of ParcelableListBinder.java , there is a possible way to steal mAllowlistToken to launch an app from background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-38034	Windows Filtering Platform Elevation of Privilege Vulnerability	7.8	More Details
CVE-2024-31320	In setSkipPrompt of AssociationRequest.java , there is a possible way to establish a companion device association without any confirmation due to CDM. 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-2024-20783	InDesign Desktop versions ID19.3, ID18.5.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-34139	Bridge versions 14.0.4, 13.0.7, 14.1 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-39069	An issue in ifood Order Manager v3.35.5 'Gestor de Peddios.exe' allows attackers to execute arbitrary code via a DLL hijacking attack.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34720	In com_android_internal_os_ZygoteCommandBuffer_nativeForkRepeatedly of com_android_internal_os_ZygoteCommandBuffer.cpp, there is a possible method to perform arbitrary code execution in any app zygote processes due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-37999	A vulnerability has been identified in Medicalis Workflow Orchestrator (All versions). The affected application executes as a trusted account with high privileges and network access. This could allow an authenticated local attacker to escalate privileges.	7.8	More Details
CVE-2024-27459	The interactive service in OpenVPN 2.6.9 and earlier allows an attacker to send data causing a stack overflow which can be used to execute arbitrary code with more privileges.	7.8	More Details
CVE-2024-20785	InDesign Desktop versions ID19.3, ID18.5.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-31339	In multiple functions of StatsService.cpp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-31335	In DevmemIntChangeSparse2 of devicemem_server.c, there is a possible arbitrary code execution due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-39479	In the Linux kernel, the following vulnerability has been resolved: drm/i915/hwmon: Get rid of devm When both hwmon and hwmon drvdata (on which hwmon depends) are device managed resources, the expectation, on device unbind, is that hwmon will be released before drvdata. However, in i915 there are two separate code paths, which both release either drvdata or hwmon and either can be released before the other. These code paths (for device unbind) are as follows (see also the bug referenced below): Call Trace: release_nodes+0x11/0x70 devres_release_group+0xb2/0x110 component_unbind_all+0x8d/0xa0 component_del+0xa5/0x140 intel_pxp_tee_component_fini+0x29/0x40 [i915] intel_pxp_fini+0x33/0x80 [i915] i915_driver_remove+0x4c/0x120 [i915] i915_pci_remove+0x19/0x30 [i915] pci_device_remove+0x32/0xa0 device_release_driver_internal+0x19c/0x200 unbind_store+0x9c/0xb0 and Call Trace: release_nodes+0x11/0x70 devres_release_all+0x8a/0xc0 device_unbind_cleanup+0x9/0x70 device_release_driver_internal+0x1c1/0x200 unbind_store+0x9c/0xb0 This means that in i915, if use devm, we cannot gurantee that hwmon will always be released before drvdata. Which means that we have a uaf if hwmon sysfs is accessed when drvdata has been released but hwmon hasn't. The only way out of this seems to be do get rid of devm_ and release/free everything explicitly during device unbind. v2: Change commit message and other minor code changes v3: Cleanup from i915_hwmon_register on error (Armin Wolf) v4: Eliminate potential static analyzer warning (Rodrigo) Eliminate fetch_and_zero (Jani) v5: Restore previous logic for ddat_gt->hwmon_dev error return (Andi)	7.8	More Details
CVE-2024-39480	In the Linux kernel, the following vulnerability has been resolved: kdb: Fix buffer overflow during tab-complete Currently, when the user attempts symbol completion with the Tab key, kdb will use strncpy() to insert the completed symbol into the command buffer. Unfortunately it passes the size of the source buffer rather than the destination to strncpy() with predictably horrible results. Most obviously if the command buffer is already full but cp, the cursor position, is in the middle of the buffer, then we will write past the end of the supplied buffer. Fix this by replacing the dubious strncpy() calls with memmove()/memcpy() calls plus explicit boundary checks to make sure we have enough space before we start moving characters around.	7.8	More Details
CVE-2023-3289	A BOLA vulnerability in POST /services allows a low privileged user to create a service for any user in the system (including admin). This results in unauthorized data manipulation.	7.7	More Details
CVE-2024-37497	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Crocoblock JetThemeCore allows File Manipulation.This issue affects JetThemeCore: from n/a before 2.2.1.	7.7	More Details
CVE-2023-3286	A BOLA vulnerability in POST /secretaries allows a low privileged user to create a low privileged user (secretary) in the system. This results in unauthorized data manipulation.	7.7	More Details
CVE-2024-39933	Gogs through 0.13.0 allows argument injection during the tagging of a new release.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39592	Elements of PDCE does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This allows an attacker to read sensitive information causing high impact on the confidentiality of the application.	7.7	More Details
CVE-2023-3285	A BOLA vulnerability in POST /appointments allows a low privileged user to create an appointment for any user in the system (including admin). This results in unauthorized data manipulation.	7.7	More Details
CVE-2024-37486	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Paid Memberships Pro.This issue affects Paid Memberships Pro: from n/a through 3.0.5.	7.6	More Details
CVE-2024-27783	Multiple cross-site request forgery (CSRF) vulnerabilities [CWE-352] in FortiAIOps version 2.0.0 may allow an unauthenticated remote attacker to perform arbitrary actions on behalf of an authenticated user via tricking the victim to execute malicious GET requests.	7.6	More Details
CVE-2024-35266	Azure DevOps Server Spoofing Vulnerability	7.6	More Details
CVE-2024-37256	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Tutor LMS.This issue affects Tutor LMS: from n/a through 2.7.1.	7.6	More Details
CVE-2024-35267	Azure DevOps Server Spoofing Vulnerability	7.6	More Details
CVE-2024-39867	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected devices do not properly validate the authentication when performing certain actions in the web interface allowing an unauthenticated attacker to access and edit device configuration information of devices for which they have no privileges.	7.6	More Details
CVE-2024-39868	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected devices do not properly validate the authentication when performing certain actions in the web interface allowing an unauthenticated attacker to access and edit VxLAN configuration information of networks for which they have no privileges.	7.6	More Details
CVE-2024-29511	Artifex Ghostscript before 10.03.1, when Tesseract is used for OCR, has a directory traversal issue that allows arbitrary file reading (and writing of error messages to arbitrary files) via OCRLanguage. For example, exploitation can use debug_file /tmp/out and user_patterns_file /etc/passwd.	7.5	More Details
CVE-2024-35227	Discourse is an open-source discussion platform. Prior to version 3.2.3 on the `stable` branch and version 3.3.0.beta3 on the `tests-passed` branch, Oneboxing against a carefully crafted malicious URL can reduce the availability of a Discourse instance. The problem has been patched in version 3.2.3 on the `stable` branch and version 3.3.0.beta3 on the `tests-passed` branch. There are no known workarounds available for this vulnerability.	7.5	More Details
CVE-2024-38078	Xbox Wireless Adapter Remote Code Execution Vulnerability	7.5	More Details
CVE-2024-38073	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	7.5	More Details
CVE-2024-38072	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	7.5	More Details
CVE-2024-39873	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application does not properly implement brute force protection against user credentials in its web API. This could allow an attacker to learn user credentials that are vulnerable to brute force attacks.	7.5	More Details
CVE-2024-38071	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39874	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application does not properly implement brute force protection against user credentials in its Client Communication component. This could allow an attacker to learn user credentials that are vulnerable to brute force attacks.	7.5	More Details
CVE-2023-52237	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC, RUGGEDCOM i802, RUGGEDCOM i802NC, RUGGEDCOM i803, RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM M2100NC, RUGGEDCOM M2200, RUGGEDCOM M2200NC, RUGGEDCOM M969, RUGGEDCOM M969NC, RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC, RUGGEDCOM RS400, RUGGEDCOM RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC, RUGGEDCOM RS416, RUGGEDCOM RS416NC, RUGGEDCOM RS416NCv2 V4.X, RUGGEDCOM RS416NCv2 V5.X, RUGGEDCOM RS416P, RUGGEDCOM RS416PNC, RUGGEDCOM RS416PNCv2 V4.X, RUGGEDCOM RS416PNCv2 V5.X, RUGGEDCOM RS416Pv2 V4.X, RUGGEDCOM RS416Pv2 V5.X, RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC, RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GNC, RUGGEDCOM RS900GNC(32M) V4.X, RUGGEDCOM RS900GNC(32M) V5.X, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPNC, RUGGEDCOM RS900L, RUGGEDCOM RS900LNC, RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-GETS-XX, RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM RS900MNC-STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM RS900NC(32M) V4.X, RUGGEDCOM RS900NC(32M) V5.X, RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GNC, RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200NC, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300NC V4.X, RUGGEDCOM RSG2300NC V5.X, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488NC V4.X, RUGGEDCOM RSG2488NC V5.X, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM RSL910, RUGGEDCOM RSL910NC, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. The web server of the affected devices allow a low privileged user to access hashes and password salts of all system's users, including admin users. An attacker could use the obtained information to brute force the passwords offline.	7.5	More Details
CVE-2024-6427	Uncontrolled Resource Consumption vulnerability in MESbook 20221021.03 version. An unauthenticated remote attacker can use the "message" parameter to inject a payload with dangerous JavaScript code, causing the application to loop requests on itself, which could lead to resource consumption and disable the application.	7.5	More Details
CVE-2024-38061	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability	7.5	More Details
CVE-2024-39888	A vulnerability has been identified in Mendix Encryption (All versions >= V10.0.0 < V10.0.2). Affected versions of the module define a specific hard-coded default value for the EncryptionKey constant, which is used in projects where no individual EncryptionKey was specified. This could allow to an attacker to decrypt any encrypted project data, as the default encryption key can be considered compromised.	7.5	More Details
CVE-2024-38015	Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability	7.5	More Details
CVE-2024-37419	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Codeless Cowidgets – Elementor Addons allows Path Traversal.This issue affects Cowidgets – Elementor Addons: from n/a through 1.1.1.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39689	Certifi is a curated collection of Root Certificates for validating the trustworthiness of SSL certificates while verifying the identity of TLS hosts. Certifi starting in 2021.05.30 and prior to 2024.07.4 recognized root certificates from `GLOBALTRUST`. Certifi 2024.07.04 removes root certificates from `GLOBALTRUST` from the root store. These are in the process of being removed from Mozilla's trust store. `GLOBALTRUST`'s root certificates are being removed pursuant to an investigation which identified "long-running and unresolved compliance issues."	7.5	More Details
CVE-2024-34750	Improper Handling of Exceptional Conditions, Uncontrolled Resource Consumption vulnerability in Apache Tomcat. When processing an HTTP/2 stream, Tomcat did not handle some cases of excessive HTTP headers correctly. This led to a miscounting of active HTTP/2 streams which in turn led to the use of an incorrect infinite timeout which allowed connections to remain open which should have been closed. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1 through 10.1.24, from 9.0.0-M1 through 9.0.89. Users are recommended to upgrade to version 11.0.0-M21, 10.1.25 or 9.0.90, which fixes the issue.	7.5	More Details
CVE-2024-38031	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability	7.5	More Details
CVE-2024-38068	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability	7.5	More Details
CVE-2024-38067	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability	7.5	More Details
CVE-2024-37224	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in smartypants SP Project & Document Manager.This issue affects SP Project & Document Manager: from n/a through 4.71.	7.5	More Details
CVE-2024-38064	Windows TCP/IP Information Disclosure Vulnerability	7.5	More Details
CVE-2024-6604	Memory safety bugs present in Firefox 127, Firefox ESR 115.12, and Thunderbird 115.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 128, Firefox ESR < 115.13, Thunderbird < 115.13, and Thunderbird < 128.	7.5	More Details
CVE-2024-38453	The Avalara for Salesforce CPQ app before 7.0 for Salesforce allows attackers to read an API key. NOTE: the current version is 11 as of mid-2024.	7.5	More Details
CVE-2024-31504	Buffer Overflow vulnerability in SILA Embedded Solutions GmbH freemodbus v.2018-09-12 allows a remtoe attacker to cause a denial of service via the LINUXTCP server component.	7.5	More Details
CVE-2024-6563	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in Renesas arm-trusted-firmware allows Local Execution of Code. This vulnerability is associated with program files https://github.Com/renesas-rcar/arm-trusted-firmware/blob/rcar_gen3_v2.5/drivers/renesas/common/io/i... https://github.Com/renesas-rcar/arm-trusted-firmware/blob/rcar_gen3_v2.5/drivers/renesas/common/io/io_rcar.C . In line 313 "addr_loaded_cnt" is checked not to be "CHECK_IMAGE_AREA_CNT" (5) or larger, this check does not halt the function. Immediately after (line 317) there will be an overflow in the buffer and the value of "dst" will be written to the area immediately after the buffer, which is "addr_loaded_cnt". This will allow an attacker to freely control the value of "addr_loaded_cnt" and thus control the destination of the write immediately after (line 318). The write in line 318 will then be fully controlled by said attacker, with whichever address and whichever value ("len") they desire.	7.5	More Details
CVE-2024-39698	electron-updater allows for automatic updates for Electron apps. The file `packages/electron-updater/src/windowsExecutableCodeSignatureVerifier.ts` implements the signature validation routine for Electron applications on Windows. Because of the surrounding shell, a first pass by `cmd.exe` expands any environment variable found in command-line above. This creates a situation where `verifySignature()` can be tricked into validating the certificate of a different file than the one that was just downloaded. If the step is successful, the malicious update will be executed even if its signature is invalid. This attack assumes a compromised update manifest (server compromise, Man-in-the-Middle attack if fetched over HTTP, Cross-Site Scripting to point the application to a malicious updater server, etc.). The patch is available starting from 6.3.0-alpha.6.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38095	.NET and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2024-24974	The interactive service in OpenVPN 2.6.9 and earlier allows the OpenVPN service pipe to be accessed remotely, which allows a remote attacker to interact with the privileged OpenVPN interactive service.	7.5	More Details
CVE-2024-39027	SeaCMS v12.9 has an unauthorized SQL injection vulnerability. The vulnerability is caused by the SQL injection through the cid parameter at /js/player/dmplayer/dmku/index.php?ac=edit, which can cause sensitive database information to be leaked.	7.5	More Details
CVE-2024-39210	Best House Rental Management System v1.0 was discovered to contain an arbitrary file read vulnerability via the Page parameter at index.php. This vulnerability allows attackers to read arbitrary PHP files and access other sensitive information within the application.	7.5	More Details
CVE-2024-40597	An issue was discovered in the CheckUser extension for MediaWiki through 1.42.1. It can expose suppressed information for log events. (The log_deleted attribute is not respected.)	7.5	More Details
CVE-2024-38112	Windows MSHTML Platform Spoofing Vulnerability	7.5	More Details
CVE-2024-30098	Windows Cryptographic Services Security Feature Bypass Vulnerability	7.5	More Details
CVE-2024-5971	A vulnerability was found in Undertow, where the chunked response hangs after the body was flushed. The response headers and body were sent but the client would continue waiting as Undertow does not send the expected 0\r\n termination of the chunked response. This results in uncontrolled resource consumption, leaving the server side to a denial of service attack. This happens only with Java 17 TLSv1.3 scenarios.	7.5	More Details
CVE-2024-6227	A vulnerability in aimhubio/aim version 3.19.3 allows an attacker to cause an infinite loop by configuring the remote tracking server to point at itself. This results in the server endlessly connecting to itself, rendering it unable to respond to other connections.	7.5	More Details
CVE-2024-37767	Insecure permissions in the component /api/admin/user of 14Finger v1.1 allows attackers to access all user information via a crafted GET request.	7.5	More Details
CVE-2023-52340	The IPv6 implementation in the Linux kernel before 6.3 has a net/ipv6/route.c max_size threshold that can be consumed easily, e.g., leading to a denial of service (network is unreachable errors) when IPv6 packets are sent in a loop via a raw socket.	7.5	More Details
CVE-2024-36676	Incorrect access control in BookStack before v24.05.1 allows attackers to confirm existing system users and perform targeted notification email DoS via public facing forms.	7.5	More Details
CVE-2024-39896	Directus is a real-time API and App dashboard for managing SQL database content. When relying on SSO providers in combination with local authentication it can be possible to enumerate existing SSO users in the instance. This is possible because if an email address exists in Directus and belongs to a known SSO provider then it will throw a "helpful" error that the user belongs to another provider. This vulnerability is fixed in 10.13.0.	7.5	More Details
CVE-2024-38091	Microsoft WS-Discovery Denial of Service Vulnerability	7.5	More Details
CVE-2024-32987	Microsoft SharePoint Server Information Disclosure Vulnerability	7.5	More Details
CVE-2024-39321	Traefik is an HTTP reverse proxy and load balancer. Versions prior to 2.11.6, 3.0.4, and 3.1.0-rc3 have a vulnerability that allows bypassing IP allow-lists via HTTP/3 early data requests in QUIC 0-RTT handshakes sent with spoofed IP addresses. Versions 2.11.6, 3.0.4, and 3.1.0-rc3 contain a patch for this issue. No known workarounds are available.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30105	.NET and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2024-39182	An information disclosure vulnerability in ISPmanager v6.98.0 allows attackers to access sensitive details of the root user's session via an arbitrary command (ISP6-1779).	7.5	More Details
CVE-2024-33862	A buffer-management vulnerability in OPC Foundation OPCFoundation.NetStandard.Opc.Ua.Core before 1.05.374.54 could allow remote attackers to exhaust memory resources. It is triggered when the system receives an excessive number of messages from a remote source. This could potentially lead to a denial of service (DoS) condition, disrupting the normal operation of the system.	7.5	More Details
CVE-2024-3651	A vulnerability was identified in the kjd/idna library, specifically within the `idna.encode()` function, affecting version 3.6. The issue arises from the function's handling of crafted input strings, which can lead to quadratic complexity and consequently, a denial of service condition. This vulnerability is triggered by a crafted input that causes the `idna.encode()` function to process the input with considerable computational load, significantly increasing the processing time in a quadratic manner relative to the input size.	7.5	More Details
CVE-2023-50178	An improper certificate validation vulnerability [CWE-295] in FortiADC 7.4.0, 7.2.0 through 7.2.3, 7.1 all versions, 7.0 all versions, 6.2 all versions, 6.1 all versions and 6.0 all versions may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and various remote servers such as private SDN connectors and FortiToken Cloud.	7.4	More Details
CVE-2024-6603	In an out-of-memory scenario an allocation could fail but free would have been called on the pointer afterwards leading to memory corruption. This vulnerability affects Firefox < 128, Firefox ESR < 115.13, Thunderbird < 115.13, and Thunderbird < 128.	7.4	More Details
CVE-2024-30061	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	7.3	More Details
CVE-2024-38081	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability	7.3	More Details
CVE-2024-38033	PowerShell Elevation of Privilege Vulnerability	7.3	More Details
CVE-2024-31331	In setMimeGroup of PackageManagerService.java, there is a possible way to hide the service from Settings due to a logic error in the code. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2024-31324	In hide of WindowState.java, there is a possible way to bypass tapjacking/overlay protection by launching the activity in portrait mode first and then rotating it to landscape mode. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2024-38044	DHCP Server Service Remote Code Execution Vulnerability	7.2	More Details
CVE-2024-39687	Fedify is a TypeScript library for building federated server apps powered by ActivityPub and other standards. At present, when Fedify needs to retrieve an object or activity from a remote activitypub server, it makes a HTTP request to the `@id` or other resources present within the activity it has received from the web. This activity could reference an `@id` that points to an internal IP address, allowing an attacker to send request to resources internal to the fedify server's network. This applies to not just resolution of documents containing activities or objects, but also to media URLs as well. Specifically this is a Server Side Request Forgery attack. Users should upgrade to Fedify version 0.9.2, 0.10.1, or 0.11.1 to receive a patch for this issue.	7.2	More Details
CVE-2024-37260	Server-Side Request Forgery (SSRF) vulnerability in Theme-Ruby Foxiz.This issue affects Foxiz: from n/a through 2.3.5.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38019	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability	7.2	More Details
CVE-2024-21778	A heap-based buffer overflow vulnerability exists in the configuration file mib_init_value_array functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted .dat file can lead to arbitrary code execution. An attacker can upload a malicious file to trigger this vulnerability.	7.2	More Details
CVE-2023-50383	Three os command injection vulnerabilities exist in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `localPin` request's parameter.	7.2	More Details
CVE-2023-50382	Three os command injection vulnerabilities exist in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `peerPin` request's parameter.	7.2	More Details
CVE-2024-38023	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2023-50381	Three os command injection vulnerabilities exist in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `targetAPSsid` request's parameter.	7.2	More Details
CVE-2023-50330	A stack-based buffer overflow vulnerability exists in the boa getInfo functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger this vulnerability.	7.2	More Details
CVE-2024-38024	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2024-38025	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability	7.2	More Details
CVE-2023-50243	Two stack-based buffer overflow vulnerabilities exist in the boa formIpQoS functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `comment` request's parameter.	7.2	More Details
CVE-2024-4341	Improper Privilege Management vulnerability in Ekstrem Bir Bilgisayar Danismanlik Ic Ve Dis Ticaret Ltd. Sti. Extreme XDS allows Collect Data as Provided by Users.This issue affects Extreme XDS: before 3928.	7.2	More Details
CVE-2023-50240	Two stack-based buffer overflow vulnerabilities exist in the boa set_RadvdInterfaceParam functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `AdvDefaultPreference` request's parameter.	7.2	More Details
CVE-2023-50239	Two stack-based buffer overflow vulnerabilities exist in the boa set_RadvdInterfaceParam functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `interfacename` request's parameter.	7.2	More Details
CVE-2023-49867	A stack-based buffer overflow vulnerability exists in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger this vulnerability.	7.2	More Details
CVE-2023-49595	A stack-based buffer overflow vulnerability exists in the boa rollback_control_code functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49593	Leftover debug code exists in the boa formSysCmd functionality of LevelOne WBR-6013 RER4_A_v3411b_2T2R_LEV_09_170623. A specially crafted network request can lead to arbitrary command execution.	7.2	More Details
CVE-2024-5672	A high privileged remote attacker can execute arbitrary system commands via GET requests due to improper neutralization of special elements used in an OS command.	7.2	More Details
CVE-2023-49073	A stack-based buffer overflow vulnerability exists in the boa formFilter functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability.	7.2	More Details
CVE-2023-48270	A stack-based buffer overflow vulnerability exists in the boa formDnsv6 functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability.	7.2	More Details
CVE-2023-47856	A stack-based buffer overflow vulnerability exists in the boa set_RadvdPrefixParam functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.	7.2	More Details
CVE-2023-45742	An integer overflow vulnerability exists in the boa updateConfigIntoFlash functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability.	7.2	More Details
CVE-2023-45215	A stack-based buffer overflow vulnerability exists in the boa setRepeaterSsid functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability.	7.2	More Details
CVE-2023-41251	A stack-based buffer overflow vulnerability exists in the boa formRoute functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send an HTTP request to trigger this vulnerability.	7.2	More Details
CVE-2024-38028	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability	7.2	More Details
CVE-2023-34435	A firmware update vulnerability exists in the boa formUpload functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted network packets can lead to arbitrary firmware update. An attacker can provide a malicious file to trigger this vulnerability.	7.2	More Details
CVE-2023-50244	Two stack-based buffer overflow vulnerabilities exist in the boa formIpQoS functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `entry_name` request's parameter.	7.2	More Details
CVE-2024-35154	IBM WebSphere Application Server 8.5 and 9.0 could allow a remote authenticated attacker, who has authorized access to the administrative console, to execute arbitrary code. Using specially crafted input, the attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 292641.	7.2	More Details
CVE-2024-6123	The Bit Form plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'iconUpload' function in all versions up to, and including, 2.13.3. This makes it possible for authenticated attackers, with administrator-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2024-38094	Microsoft SharePoint Remote Code Execution Vulnerability	7.2	More Details
CVE-2024-39597	In SAP Commerce, a user can misuse the forgotten password functionality to gain access to a Composable Storefront B2B site for which early login and registration is activated, without requiring the merchant to approve the account beforehand. If the site is not configured as isolated site, this can also grant access to other non-isolated early login sites, even if registration is not enabled for those other sites.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6180	The EventON plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'eventon_import_settings' ajax action in all versions up to, and including, 2.2.15. This makes it possible for unauthenticated attackers to update plugin settings, including adding stored cross-site scripting to settings options displayed on event calendar pages.	7.2	More Details
CVE-2024-5974	A buffer overflow in WatchGuard Fireware OS could may allow an authenticated remote attacker with privileged management access to execute arbitrary code with system privileges on the firewall. This issue affects Fireware OS: from 11.9.6 through 12.10.3.	7.2	More Details
CVE-2024-28748	A remote attacker with high privileges may use a reading file function to inject OS commands.	7.2	More Details
CVE-2024-28749	A remote attacker with high privileges may use a writing file function to inject OS commands.	7.2	More Details
CVE-2024-28750	A remote attacker with high privileges may use a deleting file function to inject OS commands.	7.2	More Details
CVE-2024-5479	The Easy Pixels plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin settings in all versions up to, and including, 2.13 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2024-30081	Windows NTLM Spoofing Vulnerability	7.1	More Details
CVE-2024-37472	Cross Site Scripting (XSS) vulnerability in WofficeIO Woffice allows Reflected XSS.This issue affects Woffice: from n/a through 5.4.8.	7.1	More Details
CVE-2024-38032	Microsoft Xbox Remote Code Execution Vulnerability	7.1	More Details
CVE-2024-37471	Cross Site Scripting (XSS) vulnerability in WofficeIO Woffice Core allows Reflected XSS.This issue affects Woffice Core: from n/a through 5.4.8.	7.1	More Details
CVE-2024-39487	In the Linux kernel, the following vulnerability has been resolved: bonding: Fix out-of-bounds read in bond_option_arp_ip_targets_set() In function bond_option_arp_ip_targets_set(), if newval->string is an empty string, newval->string+1 will point to the byte after the string, causing an out-of-bound read. BUG: KASAN: slab-out-of-bounds in strlen+0x7d/0xa0 lib/string.c:418 Read of size 1 at addr ffff8881119c4781 by task syz-executor665/8107 CPU: 1 PID: 8107 Comm: syz-executor665 Not tainted 6.7.0-rc7 #1 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xd9/0x150 lib/dump_stack.c:106 print_address_description mm/kasan/report.c:364 [inline] print_report+0xc1/0x5e0 mm/kasan/report.c:475 kasan_report+0xbe/0xf0 mm/kasan/report.c:588 strlen+0x7d/0xa0 lib/string.c:418 __fortify_strlen include/linux/fortify-string.h:210 [inline] in4_pton+0xa3/0x3f0 net/core/utils.c:130 bond_option_arp_ip_targets_set+0xc2/0x910 drivers/net/bonding/bond_options.c:1201 __bond_opt_set+0x2a4/0x1030 drivers/net/bonding/bond_options.c:767 __bond_opt_set_notify+0x48/0x150 drivers/net/bonding/bond_options.c:792 bond_opt_tryset_rtnl+0xda/0x160 drivers/net/bonding/bond_options.c:817 bonding_sysfs_store_option+0xa1/0x120 drivers/net/bonding/bond_sysfs.c:156 dev_attr_store+0x54/0x80 drivers/base/core.c:2366 sysfs_kf_write+0x114/0x170 fs/sysfs/file.c:136 kernfs_fop_write_iter+0x337/0x500 fs/kernfs/file.c:334 call_write_iter include/linux/fs.h:2020 [inline] new_sync_write fs/read_write.c:491 [inline] vfs_write+0x96a/0xd80 fs/read_write.c:584 ksys_write+0x122/0x250 fs/read_write.c:637 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0x40/0x110 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b ---[end trace]--- Fix it by adding a check of string length before using it.	7.1	More Details
CVE-2024-34724	In _UnrefAndMaybeDestroy of pmr.c, there is a possible arbitrary code execution due to a race condition. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34725	In DevmemIntUnexportCtx of devicemem_server.c, there is a possible arbitrary code execution due to a race condition. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.0	More Details
CVE-2024-34123	Premiere Pro versions 23.6.5, 24.4.1 and earlier are affected by an Untrusted Search Path vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by inserting a malicious file into the search path, which the application might execute instead of the legitimate file. This could occur when the application uses a search path to locate executables or libraries. Exploitation of this issue requires user interaction, attack complexity is high.	7.0	More Details
CVE-2024-38022	Windows Image Acquisition Elevation of Privilege Vulnerability	7.0	More Details
CVE-2024-39486	In the Linux kernel, the following vulnerability has been resolved: drm/drm_file: Fix pid refcounting race <maarten.lankhorst@linux.intel.com>, Maxime Ripard <mripard@kernel.org>, Thomas Zimmermann <tzimmermann@suse.de> filp->pid is supposed to be a refcounted pointer; however, before this patch, drm_file_update_pid() only increments the refcount of a struct pid after storing a pointer to it in filp->pid and dropping the dev->filelist_mutex, making the following race possible: process A process B ========= ========= begin drm_file_update_pid mutex_lock(&dev->filelist_mutex) rcu_replace_pointer(filp->pid, <pid B>, 1) mutex_unlock(&dev->filelist_mutex) begin drm_file_update_pid mutex_lock(&dev->filelist_mutex) rcu_replace_pointer(filp->pid, <pid A>, 1) mutex_unlock(&dev->filelist_mutex) get_pid(<pid A>) synchronize_rcu() put_pid(<pid B>) *** pid B reaches refcount 0 and is freed here *** get_pid(<pid B>) *** UAF *** synchronize_rcu() put_pid(<pid A>) As far as I know, this race can only occur with CONFIG_PREEMPT_RCU=y because it requires RCU to detect a quiescent state in code that is not explicitly calling into the scheduler. This race leads to use-after-free of a "struct pid". It is probably somewhat hard to hit because process A has to pass through a synchronize_rcu() operation while process B is between mutex_unlock() and get_pid(). Fix it by ensuring that by the time a pointer to the current task's pid is stored in the file, an extra reference to the pid has been taken. This fix also removes the condition for synchronize_rcu(); I think that optimization is unnecessary complexity, since in that case we would usually have bailed out on the lockless check above.	7.0	More Details
CVE-2024-1182	Uncontrolled Search Path Element vulnerability in ICONICS GENESIS64 all versions, Mitsubishi Electric GENESIS64 all versions and Mitsubishi Electric MC Works64 all versions allows a local attacker to execute a malicious code by storing a specially crafted DLL in a specific folder when GENESIS64 and MC Works64 are installed with the Pager agent in the alarm multi-agent notification feature.	7.0	More Details
CVE-2024-31327	In multiple functions of MessageQueueBase.h, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.0	More Details
CVE-2024-38069	Windows Enroll Engine Security Feature Bypass Vulnerability	7.0	More Details
CVE-2024-38330	IBM System Management for i 7.2, 7.3, and 7.4 could allow a local user to gain elevated privileges due to an unqualified library program call. A malicious actor could cause user-controlled code to run with administrator privilege. IBM X-Force ID: 295227.	7.0	More Details
CVE-2024-6222	In Docker Desktop before v4.29.0, an attacker who has gained access to the Docker Desktop VM through a container breakout can further escape to the host by passing extensions and dashboard related IPC messages. Docker Desktop v4.29.0 https://docs.docker.com/desktop/release-notes/#4290 fixes the issue on MacOS, Linux and Windows with Hyper-V backend. As exploitation requires "Allow only extensions distributed through the Docker Marketplace" to be disabled, Docker Desktop v4.31.0 https://docs.docker.com/desktop/release-notes/#4310 additionally changes the default configuration to enable this setting by default.	7.0	More Details
CVE-2024-6409	A race condition vulnerability was discovered in how signals are handled by OpenSSH's server (sshd). If a remote attacker does not authenticate within a set time period, then sshd's SIGALRM handler is called asynchronously. However, this signal handler calls various functions that are not async-signal-safe, for example, syslog(). As a consequence of a successful attack, in the worst case scenario, an attacker may be able to perform a remote code execution (RCE) as an unprivileged user running the sshd server.	7.0	More Details
CVE-2024-39593	SAP Landscape Management allows an authenticated user to read confidential data disclosed by the REST Provider Definition response. Successful exploitation can cause high impact on confidentiality of the managed entities.	6.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6505	A flaw was found in the virtio-net device in QEMU. When enabling the RSS feature on the virtio-net network card, the indirections_table data within RSS becomes controllable. Setting excessively large values may cause an index out-of-bounds issue, potentially resulting in heap overflow access. This flaw allows a privileged user in the guest to crash the QEMU process on the host.	6.8	More Details
CVE-2024-38471	Multiple TP-LINK products allow a network-adjacent attacker with an administrative privilege to execute arbitrary OS commands by restoring a crafted backup file. The affected device, with the initial configuration, allows login only from the LAN port or Wi-Fi.	6.8	More Details
CVE-2024-38065	Secure Boot Security Feature Bypass Vulnerability	6.8	More Details
CVE-2024-37726	Insecure Permissions vulnerability in Micro-Star International Co., Ltd MSI Center v.2.0.36.0 allows a local attacker to escalate privileges via the Export System Info function in MSI.CentralServer.exe	6.8	More Details
CVE-2024-2177	A Cross Window Forgery vulnerability exists within GitLab CE/EE affecting all versions from 16.3 prior to 16.11.5, 17.0 prior to 17.0.3, and 17.1 prior to 17.1.1. This condition allows for an attacker to abuse the OAuth authentication flow via a crafted payload.	6.8	More Details
CVE-2024-26184	Secure Boot Security Feature Bypass Vulnerability	6.8	More Details
CVE-2024-38058	BitLocker Security Feature Bypass Vulnerability	6.8	More Details
CVE-2024-38013	Microsoft Windows Server Backup Elevation of Privilege Vulnerability	6.7	More Details
CVE-2024-27385	A vulnerability was discovered in the slsi_handle_nan_rx_event_log_ind function in Samsung Mobile Processor Exynos 1380 and Exynos 1480 related to no input validation check on tag_len for rx coming from userspace, which can lead to heap overwrite.	6.7	More Details
CVE-2024-27386	A vulnerability was discovered in the slsi_handle_nan_rx_event_log_ind function in Samsung Mobile Processor Exynos 1380 and Exynos 1480 related to no input validation check on tag_len for tx coming from userspace, which can lead to heap overwrite.	6.7	More Details
CVE-2024-6564	Buffer overflow in "rcar_dev_init" due to using due to using untrusted data (rcar_image_number) as a loop counter before verifying it against RCAR_MAX_BL3X_IMAGE. This could lead to a full bypass of secure boot.	6.7	More Details
CVE-2024-1574	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in the licensing feature of ICONICS GENESIS64 versions 10.97 to 10.97.2, Mitsubishi Electric GENESIS64 versions 10.97 to 10.97.2 and Mitsubishi Electric MC Works64 all versions allows a local attacker to execute a malicious code with administrative privileges by tampering with a specific file that is not protected by the system.	6.7	More Details
CVE-2024-38049	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38278	A vulnerability has been identified in RUGGEDCOM RMC8388 V5.X (All versions < V5.9.0), RUGGEDCOM RMC8388NC V5.X (All versions < V5.9.0), RUGGEDCOM RS416NCv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416PNCv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416Pv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416v2 V5.X (All versions < V5.9.0), RUGGEDCOM RS900 (32M) V5.X (All versions < V5.9.0), RUGGEDCOM RS900G (32M) V5.X (All versions < V5.9.0), RUGGEDCOM RS900GNC(32M) V5.X (All versions < V5.9.0), RUGGEDCOM RS900NC(32M) V5.X (All versions < V5.9.0), RUGGEDCOM RSG2100 (32M) V5.X (All versions < V5.9.0), RUGGEDCOM RSG2100NC(32M) V5.X (All versions < V5.9.0), RUGGEDCOM RSG2288 V5.X (All versions < V5.9.0), RUGGEDCOM RSG2288NC V5.X (All versions < V5.9.0), RUGGEDCOM RSG2300 V5.X (All versions < V5.9.0), RUGGEDCOM RSG2300NC V5.X (All versions < V5.9.0), RUGGEDCOM RSG2300P V5.X (All versions < V5.9.0), RUGGEDCOM RSG2300PNC V5.X (All versions < V5.9.0), RUGGEDCOM RSG2488 V5.X (All versions < V5.9.0), RUGGEDCOM RSG2488NC V5.X (All versions < V5.9.0), RUGGEDCOM RSG907R (All versions < V5.9.0), RUGGEDCOM RSG908C (All versions < V5.9.0), RUGGEDCOM RSG909R (All versions < V5.9.0), RUGGEDCOM RSG910C (All versions < V5.9.0), RUGGEDCOM RSG920P V5.X (All versions < V5.9.0), RUGGEDCOM RSG920PNC V5.X (All versions < V5.9.0), RUGGEDCOM RSL910 (All versions < V5.9.0), RUGGEDCOM RSL910NC (All versions < V5.9.0), RUGGEDCOM RST2228 (All versions < V5.9.0), RUGGEDCOM RST2228P (All versions < V5.9.0), RUGGEDCOM RST916C (All versions < V5.9.0), RUGGEDCOM RST916P (All versions < V5.9.0). The affected products with IP forwarding enabled wrongly make available certain remote services in non-managed VLANs, even if these services are not intentionally activated. An attacker could leverage this vulnerability to create a remote shell to the affected system.	6.6	More Details
CVE-2024-39569	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 HF1). The system service of affected applications is vulnerable to command injection due to missing server side input sanitation when loading VPN configurations. This could allow an administrative remote attacker running a corresponding SINEMA Remote Connect Server to execute arbitrary code with system privileges on the client system.	6.6	More Details
CVE-2024-38020	Microsoft Outlook Spoofing Vulnerability	6.5	More Details
CVE-2024-39895	Directus is a real-time API and App dashboard for managing SQL database content. A denial of service (DoS) attack by field duplication in GraphQL is a type of attack where an attacker exploits the flexibility of GraphQL to overwhelm a server by requesting the same field multiple times in a single query. This can cause the server to perform redundant computations and consume excessive resources, leading to a denial of service for legitimate users. Request to the endpoint /graphql are sent when visualizing graphs generated at a dashboard. By modifying the data sent and duplicating many times the fields a DoS attack is possible. This vulnerability is fixed in 10.12.0.	6.5	More Details
CVE-2024-40601	An issue was discovered in the MediaWikiChat extension for MediaWiki through 1.42.1. CSRF can occur in API modules.	6.5	More Details
CVE-2024-37520	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in RadiusTheme ShopBuilder – Elementor WooCommerce Builder Addons allows Path Traversal.This issue affects ShopBuilder – Elementor WooCommerce Builder Addons: from n/a through 2.1.12.	6.5	More Details
CVE-2024-37553	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Axelerant Testimonials Widget allows Stored XSS.This issue affects Testimonials Widget: from n/a through 4.0.4.	6.5	More Details
CVE-2024-6052	Stored XSS in Checkmk before versions 2.3.0p8, 2.2.0p29, 2.1.0p45, and 2.0.0 (EOL) allows users to execute arbitrary scripts by injecting HTML elements	6.5	More Details
CVE-2024-38105	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	6.5	More Details
CVE-2024-37474	Cross Site Scripting (XSS) vulnerability in Automattic Newspack Ads allows Stored XSS.This issue affects Newspack Ads: from n/a through 1.47.1.	6.5	More Details
CVE-2024-5992	The Cliengo – Chatbot plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_chatbot_token' and 'update_chatbot_position' functions in all versions up to, and including, 3.0.1. This makes it possible for unauthenticated attackers to change chatbot settings, which can lead to unavailability or other changes to the chatbot.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37547	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Livemesh Livemesh Addons for Elementor.This issue affects Livemesh Addons for Elementor: from n/a through 8.4.0.	6.5	More Details
CVE-2024-37476	Cross Site Scripting (XSS) vulnerability in Automattic Newspack Campaigns allows Stored XSS.This issue affects Newspack Campaigns: from n/a through 2.31.1.	6.5	More Details
CVE-2024-37554	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CodeAstrology Team UltraAddons Elementor Lite (Header & Footer Builder, Menu Builder, Cart Icon, Shortcode).This issue affects UltraAddons Elementor Lite (Header & Footer Builder, Menu Builder, Cart Icon, Shortcode): from n/a through 1.1.6.	6.5	More Details
CVE-2024-38030	Windows Themes Spoofing Vulnerability	6.5	More Details
CVE-2024-37454	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in AWSM Innovations AWSM Team allows Path Traversal.This issue affects AWSM Team: from n/a through 1.3.1.	6.5	More Details
CVE-2024-27717	Cross Site Request Forgery vulnerability in Eskooly Free Online School Management Software v.3.0 and before allows a remote attacker to escalate privileges via the Token Handling component.	6.5	More Details
CVE-2024-38027	Windows Line Printer Daemon Service Denial of Service Vulnerability	6.5	More Details
CVE-2024-39220	BAS-IP AV-01D, AV-01MD, AV-01MFD, AV-01ED, AV-01KD, AV-01BD, AV-01KBD, AV-02D, AV-02IDE, AV-02IDR, AV-02IPD, AV-02FDE, AV-02FDR, AV-03D, AV-03BD, AV-04AFD, AV-04ASD, AV-04FD, AV-04SD, AV-05FD, AV-05SD, AA-07BD, AA-07BDI, BA-04BD, BA-04MD, BA-08BD, BA-08MD, BA-12BD, BA-12MD, CR-02BD before firmware v3.9.2 allows authenticated attackers to read SIP account passwords via a crafted GET request.	6.5	More Details
CVE-2024-37539	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Delower WP To Do allows Stored XSS.This issue affects WP To Do: from n/a through 1.3.0.	6.5	More Details
CVE-2024-6237	A flaw was found in the 389 Directory Server. This flaw allows an unauthenticated user to cause a systematic server crash while sending a specific extended search request, leading to a denial of service.	6.5	More Details
CVE-2024-38101	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	6.5	More Details
CVE-2024-37541	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in StaxWP Elementor Addons, Widgets and Enhancements – Stax allows Stored XSS.This issue affects Elementor Addons, Widgets and Enhancements – Stax: from n/a through 1.4.4.1.	6.5	More Details
CVE-2024-32498	An issue was discovered in OpenStack Cinder through 24.0.0, Glance before 28.0.2, and Nova before 29.0.3. Arbitrary file access can occur via custom QCOW2 external data. By supplying a crafted QCOW2 image that references a specific data file path, an authenticated user may convince systems to return a copy of that file's contents from the server, resulting in unauthorized access to potentially sensitive data. All Cinder and Nova deployments are affected; only Glance deployments with image conversion enabled are affected.	6.5	More Details
CVE-2024-39869	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected products allow to upload certificates. An authenticated attacker could upload a crafted certificates leading to a permanent denial-of-service situation. In order to recover from such an attack, the offending certificate needs to be removed manually.	6.5	More Details
CVE-2024-3332	A malicious BLE device can send a specific order of packet sequence to cause a DoS attack on the victim BLE device	6.5	More Details
CVE-2024-38048	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38102	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	6.5	More Details
CVE-2023-32735	A vulnerability has been identified in SIMATIC STEP 7 Safety V16 (All versions < V16 Update 7), SIMATIC STEP 7 Safety V17 (All versions < V17 Update 7), SIMATIC STEP 7 Safety V18 (All versions < V18 Update 2), SIMATIC STEP 7 V16 (All versions < V16 Update 7), SIMATIC STEP 7 V17 (All versions < V17 Update 7), SIMATIC STEP 7 V18 (All versions < V18 Update 2), SIMATIC WinCC Unified V16 (All versions < V16 Update 7), SIMATIC WinCC Unified V17 (All versions < V17 Update 7), SIMATIC WinCC Unified V18 (All versions < V18 Update 2), SIMATIC WinCC V16 (All versions < V16.7), SIMATIC WinCC V17 (All versions < V17.7), SIMATIC WinCC V18 (All versions < V18 Update 2), SIMOCODE ES V16 (All versions < V16 Update 7), SIMOCODE ES V17 (All versions < V17 Update 7), SIMOCODE ES V18 (All versions < V18 Update 2), SIMOTION SCOUT TIA V5.4 SP1 (All versions), SIMOTION SCOUT TIA V5.4 SP3 (All versions), SIMOTION SCOUT TIA V5.5 SP1 (All versions), SINAMICS Startdrive V16 (All versions), SINAMICS Startdrive V17 (All versions), SINAMICS Startdrive V18 (All versions), SIRIUS Safety ES V17 (All versions < V17 Update 7), SIRIUS Safety ES V18 (All versions < V18 Update 2), SIRIUS Soft Starter ES V17 (All versions < V17 Update 7), SIRIUS Soft Starter ES V18 (All versions < V18 Update 2), Soft Starter ES V16 (All versions < V16 Update 7), TIA Portal Cloud V3.0 (All versions < V18 Update 2). Affected applications do not properly restrict the .NET BinaryFormatter when deserializing hardware configuration profiles. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application. This is the same issue that exists for .NET BinaryFormatter https://docs.microsoft.com/en-us/visualstudio/code-quality/ca2300.	6.5	More Details
CVE-2024-39181	Shenzhen Libituo Technology Co., Ltd LBT-T300-T400 v3.2 was discovered to contain a buffer overflow via the ApCliSsid parameter in thegenerate_conf_router() function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	6.5	More Details
CVE-2024-37546	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in biplob018 Image Hover Effects - Caption Hover with Carousel allows Stored XSS.This issue affects Image Hover Effects - Caption Hover with Carousel: from n/a through 3.0.2.	6.5	More Details
CVE-2024-2231	The allows any authenticated user to join a private group due to a missing authorization check on a function	6.5	More Details
CVE-2024-37499	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in vCita Online Booking & Scheduling Calendar for WordPress by vcita allows Path Traversal.This issue affects Online Booking & Scheduling Calendar for WordPress by vcita: from n/a through 4.4.2.	6.5	More Details
CVE-2024-38086	Azure Kinect SDK Remote Code Execution Vulnerability	6.4	More Details
CVE-2024-4667	The Blog, Posts and Category Filter for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Post and Category Filter widget in all versions up to, and including, 1.0.3 due to insufficient input sanitization and output escaping on user supplied 'post_types' attribute. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-37157	Discourse is an open-source discussion platform. Prior to version 3.2.3 on the `stable` branch and version 3.3.0.beta4 on the `beta` and `tests-passed` branches, a malicious actor could get the FastImage library to redirect requests to an internal Discourse IP. This issue is patched in version 3.2.3 on the `stable` branch and version 3.3.0.beta4 on the `beta` and `tests-passed` branches. No known workarounds are available.	6.4	More Details
CVE-2024-22277	VMware Cloud Director Availability contains an HTML injection vulnerability. A malicious actor with network access to VMware Cloud Director Availability can craft malicious HTML tags to execute within replication tasks.	6.4	More Details
CVE-2024-6169	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘username’ parameter in all versions up to, and including, 1.5.112 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above and granted plugin setting edit permissions by an administrator, 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-2024-4482	The The Plus Addons for Elementor – Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Countdown' widget in all versions up to, and including, 5.6.1 due to insufficient input sanitization and output escaping on user supplied 'text_days' attribute. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-6263	The WP Lightbox 2 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘title’ parameter in all versions up to, and including, 3.0.6.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-6340	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown widget in all versions up to, and including, 4.10.35 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-6170	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘email’ parameter in all versions up to, and including, 1.5.112 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5937	The Simple Alert Boxes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Alert shortcode in all versions up to, and including, 1.4.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5881	The Webico Slider Flatsome Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wbc_image shortcode in all versions up to, and including, 2.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3639	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Posts Grid widget in all versions up to, and including, 8.3.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5669	The XPlainer – WooCommerce Product FAQ [WooCommerce Accordion FAQ Plugin] plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ffw_activate_template' function in all versions up to, and including, 1.6.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to store cross-site scripting that will trigger when viewing the dashboard templates or accessing FAQs.	6.4	More Details
CVE-2024-5457	The Panda Video plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘id’ parameter in all versions up to, and including, 1.4.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4868	The Extensions for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's EE Events and EE Flipbox widgets in all versions up to, and including, 2.0.31 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-4862	The WPBITS Addons For Elementor Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several widgets in all versions up to, and including, 1.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-6391	The oik plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's bw_button shortcode in all versions up to, and including, 4.10.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3603	The OSM – OpenStreetMap plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'osm_map' shortcode in all versions up to, and including, 6.0.2 due to insufficient input sanitization and output escaping on user supplied attributes such as 'theme'. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3563	The Genesis Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Sharing block in all versions up to, and including, 3.1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5946	The Squelch Tabs and Accordions Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tab' shortcode in all versions up to, and including, 0.4.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5641	The One Click Order Re-Order plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ced_ocor_save_general_setting' function in all versions up to, and including, 1.1.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change the plugin settings, including adding stored cross-site scripting.	6.4	More Details
CVE-2024-2926	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 8.3.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-3638	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Marquee Text Widget, Testimonials Widget, and Testimonial Slider widgets in all versions up to, and including, 8.3.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-39020	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/vpsApiData_deal.php?mudi=rev&nohrefStr=close	6.3	More Details
CVE-2024-29510	Artifex Ghostscript before 10.03.1 allows memory corruption, and SAFER sandbox bypass, via format string injection with a uniprint device.	6.3	More Details
CVE-2024-39870	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected applications can be configured to allow users to manage own users. A local authenticated user with this privilege could use this modify users outside of their own scope as well as to escalate privileges.	6.3	More Details
CVE-2024-22062	There is a permissions and access control vulnerability in ZXCLOUD IRAI.An attacker can elevate non-administrator permissions to administrator permissions by modifying the configuration.	6.3	More Details
CVE-2024-39871	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected applications do not properly separate the rights to edit device settings and to edit settings for communication relations. This could allow an authenticated attacker with the permission to manage devices to gain access to participant groups that the attacked does not belong to.	6.3	More Details
CVE-2024-39701	Directus is a real-time API and App dashboard for managing SQL database content. Directus >=9.23.0, <=v10.5.3 improperly handles _in, _nin operators. It evaluates empty arrays as valid so expressions like {"role": {"_in": $CURRENT_USER.some_field}} would evaluate to true allowing the request to pass. This results in Broken Access Control because the rule fails to do what it was intended to do: Pass rule if **field** matches any of the **values**. This vulnerability is fixed in 10.6.0.	6.3	More Details
CVE-2024-6471	A vulnerability classified as critical has been found in SourceCodester Online Tours & Travels Management 1.0. This affects an unknown part of the file sms_setting.php. The manipulation of the argument uname leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-270279.	6.3	More Details
CVE-2024-6600	Due to large allocation checks in Angle for GLSL shaders being too lenient an out-of-bounds access could occur when allocating more than 8192 ints in private shader memory on mac OS. This vulnerability affects Firefox < 128, Firefox ESR < 115.13, Thunderbird < 115.13, and Thunderbird < 128.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33870	An issue was discovered in Artifex Ghostscript before 10.03.1. There is path traversal (via a crafted PostScript document) to arbitrary files if the current directory is in the permitted paths. For example, there can be a transformation of ../../foo to ./../../foo and this will grant access if ./ is permitted.	6.3	More Details
CVE-2023-32737	A vulnerability has been identified in SIMATIC STEP 7 Safety V18 (All versions < V18 Update 2). Affected applications do not properly restrict the .NET BinaryFormatter when deserializing user-controllable input. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application. This is the same issue that exists for .NET BinaryFormatter https://docs.microsoft.com/en-us/visualstudio/code-quality/ca2300.	6.3	More Details
CVE-2024-31957	A vulnerability was discovered in Samsung Mobile Processors Exynos 2200 and Exynos 2400 where they lack a check for the validation of native handles, which can result in a DoS(Denial of Service) attack by unmapping an invalid length.	6.2	More Details
CVE-2024-39884	A regression in the core of Apache HTTP Server 2.4.60 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP scripts may be served instead of interpreted. Users are recommended to upgrade to version 2.4.61, which fixes this issue.	6.2	More Details
CVE-2024-21729	Inadequate input validation leads to XSS vulnerabilities in the accessiblemedia field.	6.1	More Details
CVE-2024-26278	The Custom Fields component not correctly filter inputs, leading to a XSS vector.	6.1	More Details
CVE-2024-21731	Improper handling of input could lead to an XSS vector in the StringHelper::truncate method.	6.1	More Details
CVE-2024-26279	The wrapper extensions do not correctly validate inputs, leading to XSS vectors.	6.1	More Details
CVE-2024-34685	Due to weak encoding of user-controlled input in SAP NetWeaver Knowledge Management XMLEditor which allows malicious scripts can be executed in the application, potentially leading to a Cross-Site Scripting (XSS) vulnerability. This has no impact on the availability of the application but it has a low impact on its confidentiality and integrity.	6.1	More Details
CVE-2024-40729	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/interfaces/add/.	6.1	More Details
CVE-2024-40735	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-outlets/{id}/edit/.	6.1	More Details
CVE-2024-37830	An issue in Outline <= v0.76.1 allows attackers to redirect a victim user to a malicious site via intercepting and changing the state cookie.	6.1	More Details
CVE-2024-40728	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/console-server-ports/{id}/edit/.	6.1	More Details
CVE-2024-5711	A stored Cross-Site Scripting (XSS) vulnerability exists in the stitionai/devika chat feature, allowing attackers to inject malicious payloads into the chat input. This vulnerability is due to the lack of input validation and sanitization on both the frontend and backend components of the application. Specifically, the application fails to sanitize user input in the chat feature, leading to the execution of arbitrary JavaScript code in the context of the user's browser session. This issue affects all versions of the application. The impact of this vulnerability includes the potential for stolen credentials, extraction of sensitive information from chat logs, projects, and other data accessible through the application.	6.1	More Details
CVE-2024-40730	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/interfaces/{id}/edit/.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40731	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/rear-ports/{id}/edit/.	6.1	More Details
CVE-2024-40732	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/rear-ports/add/.	6.1	More Details
CVE-2024-40733	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/front-ports/{id}/edit/.	6.1	More Details
CVE-2024-40734	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/front-ports/add/.	6.1	More Details
CVE-2024-40736	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-outlets/add.	6.1	More Details
CVE-2024-38972	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-ports/add/.	6.1	More Details
CVE-2024-40737	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/console-ports/add.	6.1	More Details
CVE-2024-40738	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/console-ports/{id}/edit/.	6.1	More Details
CVE-2024-40739	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-feeds/add.	6.1	More Details
CVE-2024-40740	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-feeds/{id}/edit/.	6.1	More Details
CVE-2024-40741	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the circuit ID parameter at /circuits/circuits/{id}/edit/.	6.1	More Details
CVE-2024-38963	Nopcommerce 4.70.1 is vulnerable to Cross Site Scripting (XSS) via the combined "AddProductReview.Title" and "AddProductReview.ReviewText" parameter(s) (Reviews) when creating a new review.	6.1	More Details
CVE-2024-40742	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the circuit ID parameter at /circuits/circuits/add.	6.1	More Details
CVE-2024-39174	A cross-site scripting (XSS) vulnerability in the Publish Article function of yzmcms v7.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into a published article.	6.1	More Details
CVE-2024-40726	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-ports/{id}/edit/.	6.1	More Details
CVE-2024-40727	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/console-server-ports/add/.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39594	SAP Business Warehouse - Business Planning and Simulation application does not sufficiently encode user controlled inputs, resulting in Reflected Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker can cause low impact on the confidentiality and integrity of the application.	6.1	More Details
CVE-2024-5652	In Docker Desktop on Windows before v4.31.0 allows a user in the docker-users group to cause a Windows Denial-of-Service through the exec-path Docker daemon config option in Windows containers mode.	6.1	More Details
CVE-2024-38959	Cross Site Scripting vulnerability in Creativeitem Academy LMS Learning Management System v.6.8.1 allows a remote attacker to execute arbitrary code and obtain sensitive information via the string parameter.	6.1	More Details
CVE-2024-6334	The Easy Table of Contents WordPress plugin before 2.0.67.1 does not sanitise and escape some of its settings, which could allow high privilege users such as editors to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed.	6.1	More Details
CVE-2024-37174	Custom CSS support option in SAP CRM WebClient UI does not sufficiently encode user-controlled inputs resulting in Cross-Site Scripting vulnerability. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application.	6.1	More Details
CVE-2024-37173	Due to insufficient input validation, SAP CRM WebClient UI allows an unauthenticated attacker to craft a URL link which embeds a malicious script. When a victim clicks on this link, the script will be executed in the victim's browser giving the attacker the ability to access and/or modify information with no effect on availability of the application.	6.1	More Details
CVE-2024-34481	drupal-wiki.com Drupal Wiki before 8.31.1 allows XSS via comments, captions, and image titles of a Wiki page.	6.1	More Details
CVE-2024-39203	A cross-site scripting (XSS) vulnerability in the Backend Theme Management module of Z-BlogPHP v1.7.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2024-27183	XSS vulnerability in DJ-HelpfulArticles component for Joomla.	6.1	More Details
CVE-2024-27363	A vulnerability was discovered in Samsung Mobile Processor Exynos 850, Exynos 9610, Exynos 980, Exynos 1280, Exynos 1380, Exynos 1330, Exynos W920, and Exynos W930 where it does not properly check a pointer address, which can lead to a Information disclosure.	6.0	More Details
CVE-2024-27360	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38867	A vulnerability has been identified in SIPROTEC 5 6MD84 (CP300) (All versions < V9.64), SIPROTEC 5 6MD85 (CP200) (All versions), SIPROTEC 5 6MD85 (CP300) (All versions < V9.64), SIPROTEC 5 6MD86 (CP200) (All versions), SIPROTEC 5 6MD86 (CP300) (All versions < V9.64), SIPROTEC 5 6MD89 (CP300) (All versions < V9.64), SIPROTEC 5 6MU85 (CP300) (All versions < V9.64), SIPROTEC 5 7KE85 (CP200) (All versions), SIPROTEC 5 7KE85 (CP300) (All versions < V9.64), SIPROTEC 5 7SA82 (CP100) (All versions), SIPROTEC 5 7SA82 (CP150) (All versions < V9.65), SIPROTEC 5 7SA84 (CP200) (All versions), SIPROTEC 5 7SA86 (CP200) (All versions), SIPROTEC 5 7SA86 (CP300) (All versions < V9.65), SIPROTEC 5 7SA87 (CP200) (All versions), SIPROTEC 5 7SA87 (CP300) (All versions < V9.65), SIPROTEC 5 7SD82 (CP100) (All versions), SIPROTEC 5 7SD82 (CP150) (All versions < V9.65), SIPROTEC 5 7SD84 (CP200) (All versions), SIPROTEC 5 7SD86 (CP200) (All versions), SIPROTEC 5 7SD86 (CP300) (All versions < V9.65), SIPROTEC 5 7SD87 (CP200) (All versions), SIPROTEC 5 7SD87 (CP300) (All versions < V9.65), SIPROTEC 5 7SJ81 (CP100) (All versions < V8.89), SIPROTEC 5 7SJ81 (CP150) (All versions < V9.65), SIPROTEC 5 7SJ82 (CP100) (All versions < V8.89), SIPROTEC 5 7SJ82 (CP150) (All versions < V9.65), SIPROTEC 5 7SJ85 (CP200) (All versions), SIPROTEC 5 7SJ85 (CP300) (All versions < V9.65), SIPROTEC 5 7SJ86 (CP200) (All versions), SIPROTEC 5 7SJ86 (CP300) (All versions < V9.65), SIPROTEC 5 7SK82 (CP100) (All versions < V8.89), SIPROTEC 5 7SK82 (CP150) (All versions < V9.65), SIPROTEC 5 7SK85 (CP200) (All versions), SIPROTEC 5 7SK85 (CP300) (All versions < V9.65), SIPROTEC 5 7SL82 (CP100) (All versions), SIPROTEC 5 7SL82 (CP150) (All versions < V9.65), SIPROTEC 5 7SL86 (CP200) (All versions), SIPROTEC 5 7SL86 (CP300) (All versions < V9.65), SIPROTEC 5 7SL87 (CP200) (All versions), SIPROTEC 5 7SL87 (CP300) (All versions < V9.65), SIPROTEC 5 7SS85 (CP200) (All versions), SIPROTEC 5 7SS85 (CP300) (All versions < V9.64), SIPROTEC 5 7ST85 (CP200) (All versions), SIPROTEC 5 7ST85 (CP300) (All versions < V9.64), SIPROTEC 5 7ST86 (CP300) (All versions < V9.64), SIPROTEC 5 7SX82 (CP150) (All versions < V9.65), SIPROTEC 5 7SX85 (CP300) (All versions < V9.65), SIPROTEC 5 7UM85 (CP300) (All versions < V9.64), SIPROTEC 5 7UT82 (CP100) (All versions), SIPROTEC 5 7UT82 (CP150) (All versions < V9.65), SIPROTEC 5 7UT85 (CP200) (All versions), SIPROTEC 5 7UT85 (CP300) (All versions < V9.65), SIPROTEC 5 7UT86 (CP200) (All versions), SIPROTEC 5 7UT86 (CP300) (All versions < V9.65), SIPROTEC 5 7UT87 (CP200) (All versions), SIPROTEC 5 7UT87 (CP300) (All versions < V9.65), SIPROTEC 5 7VE85 (CP300) (All versions < V9.64), SIPROTEC 5 7VK87 (CP200) (All versions), SIPROTEC 5 7VK87 (CP300) (All versions < V9.65), SIPROTEC 5 7VU85 (CP300) (All versions < V9.64), SIPROTEC 5 Communication Module ETH-BA-2EL (Rev.1) (All versions < V9.62 installed on CP150 and CP300 devices), SIPROTEC 5 Communication Module ETH-BA-2EL (Rev.1) (All versions installed on CP200 devices), SIPROTEC 5 Communication Module ETH-BA-2EL (Rev.1) (All versions < V8.89 installed on CP100 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (Rev. 1) (All versions installed on CP200 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (Rev. 1) (All versions < V9.62 installed on CP150 and CP300 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (Rev. 1) (All versions < V8.89 installed on CP100 devices), SIPROTEC 5 Communication Module ETH-BD-2FO (All versions < V9.62), SIPROTEC 5 Compact 7SX800 (CP050) (All versions < V9.64). The affected devices are supporting weak ciphers on several ports (443/tcp for web, 4443/tcp for DIGSI 5 and configurable port for syslog over TLS). This could allow an unauthorized attacker in a man-in-the-middle position to decrypt any data passed over to and from those ports.	5.9	More Details
CVE-2024-39677	NHibernate is an object-relational mapper for the .NET framework. A SQL injection vulnerability exists in some types implementing ILiteralType.ObjectToSQLString. Callers of these methods are exposed to the vulnerability, which includes mappings using inheritance with discriminator values; HQL queries referencing a static field of the application; users of the SqlInsertBuilder and SqlUpdateBuilder utilities, calling their AddColumn overload taking a literal value; and any direct use of the ObjectToSQLString methods for building SQL queries on the user side. This vulnerability is fixed in 5.4.9 and 5.5.2.	5.9	More Details
CVE-2024-39743	IBM MQ Operator 3.2.2 and IBM MQ Operator 2.0.24 IBM MQ Container Developer Edition is vulnerable to denial of service caused by incorrect memory de-allocation. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. IBM X-Force ID: 297172.	5.9	More Details
CVE-2024-38099	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	5.9	More Details
CVE-2024-1573	Improper Authentication vulnerability in the mobile monitoring feature of ICONICS GENESIS64 versions 10.97 to 10.97.2, Mitsubishi Electric GENESIS64 versions 10.97 to 10.97.2 and Mitsubishi Electric MC Works64 all versions allows a remote unauthenticated attacker to bypass proper authentication and log in to the system when all of the following conditions are met: * Active Directory is used in the security setting. * “Automatic log in” option is enabled in the security setting. * The IcoAnyGlass IIS Application Pool is running under an Active Directory Domain Account. * The IcoAnyGlass IIS Application Pool account is included in GENESIS64TM and MC Works64 Security and has permission to log in.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25639	Khoj is an application that creates personal AI agents. The Khoj Obsidian, Desktop and Web clients inadequately sanitize the AI model's response and user inputs. This can trigger Cross Site Scripting (XSS) via Prompt Injection from untrusted documents either indexed by the user on Khoj or read by Khoj from the internet when the user invokes the /online command. This vulnerability is fixed in 1.13.0.	5.9	More Details
CVE-2024-37865	An issue in S3Browser v.11.4.5 and v.10.9.9 and fixed in v.11.5.7 allows a remote attacker to obtain sensitive information via the S3 compatible storage component.	5.9	More Details
CVE-2024-30321	A vulnerability has been identified in SIMATIC PCS 7 V9.1 (All versions < V9.1 SP2 UC05), SIMATIC WinCC Runtime Professional V18 (All versions < V18 Update 5), SIMATIC WinCC Runtime Professional V19 (All versions < V19 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 23), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 17), SIMATIC WinCC V8.0 (All versions < V8.0 Update 5). The affected products do not properly handle certain requests to their web application, which may lead to the leak of privileged information. This could allow an unauthenticated remote attacker to retrieve information such as users and passwords.	5.9	More Details
CVE-2024-39150	vditor v.3.9.8 and before is vulnerable to Arbitrary file read via a crafted data packet.	5.9	More Details
CVE-2024-40035	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/userLevel_deal.php?mudi=add.	5.9	More Details
CVE-2024-6095	A vulnerability in the /models/apply endpoint of mudler/localai versions 2.15.0 allows for Server-Side Request Forgery (SSRF) and partial Local File Inclusion (LFI). The endpoint supports both http(s):// and file:// schemes, where the latter can lead to LFI. However, the output is limited due to the length of the error message. This vulnerability can be exploited by an attacker with network access to the LocalAI instance, potentially allowing unauthorized access to internal HTTP(s) servers and partial reading of local files. The issue is fixed in version 2.17.	5.8	More Details
CVE-2024-21993	SnapCenter versions prior to 5.0p1 are susceptible to a vulnerability which could allow an authenticated attacker to discover plaintext credentials.	5.7	More Details
CVE-2024-39683	ZITADEL is an open-source identity infrastructure tool. ZITADEL provides users the ability to list all user sessions of the current user agent (browser). Starting in version 2.53.0 and prior to versions 2.53.8, 2.54.5, and 2.55.1, due to a missing check, user sessions without that information (e.g. when created though the session service) were incorrectly listed exposing potentially other user's sessions. Versions 2.55.1, 2.54.5, and 2.53.8 contain a fix for the issue. There is no workaround since a patch is already available.	5.7	More Details
CVE-2024-31312	In multiple locations, there is a possible information leak due to a missing permission check. This could lead to local information disclosure exposing played media with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-31314	In multiple functions of ShortcutService.java, there is a possible persistent DOS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-38017	Microsoft Message Queuing Information Disclosure Vulnerability	5.5	More Details
CVE-2024-34140	Bridge versions 14.0.4, 13.0.7, 14.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-39118	Mommy Heather Advanced Backups up to v3.5.3 allows attackers to write arbitrary files via restoring a crafted back up.	5.5	More Details
CVE-2024-38056	Microsoft Windows Codecs Library Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38055	Microsoft Windows Codecs Library Information Disclosure Vulnerability	5.5	More Details
CVE-2024-38041	Windows Kernel Information Disclosure Vulnerability	5.5	More Details
CVE-2024-32673	Improper Validation of Array Index vulnerability in Samsung Open Source Walrus Webassembly runtime engine allows a segmentation fault issue. This issue affects Walrus: before 72c7230f32a0b791355bbdfc78669701024b0956.	5.5	More Details
CVE-2024-34721	In ensureFileColumns of MediaProvider.java, there is a possible disclosure of files owned by another user due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-39481	In the Linux kernel, the following vulnerability has been resolved: media: mc: Fix graph walk in media_pipeline_start The graph walk tries to follow all links, even if they are not between pads. This causes a crash with, e.g. a MEDIA_LNK_FL_ANCILLARY_LINK link. Fix this by allowing the walk to proceed only for MEDIA_LNK_FL_DATA_LINK links.	5.5	More Details
CVE-2024-6524	A vulnerability was found in ShopXO up to 6.1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file extend/base/Uploader.php. The manipulation of the argument source leads to server-side request forgery. 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-270367. NOTE: The original disclosure confuses CSRF with SSRF.	5.5	More Details
CVE-2024-39477	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: do not call vma_add_reservation upon ENOMEM sysbot reported a splat [1] on __unmap_hugepage_range(). This is because vma_needs_reservation() can return -ENOMEM if allocate_file_region_entries() fails to allocate the file_region struct for the reservation. Check for that and do not call vma_add_reservation() if that is the case, otherwise region_abort() and region_del() will see that we do not have any file_regions. If we detect that vma_needs_reservation() returned -ENOMEM, we clear the hugetlb_restore_reserve flag as if this reservation was still consumed, so free_huge_folio() will not increment the resv count. [1] https://lore.kernel.org/linux-mm/000000000004096100617c58d54@google.com/T/#ma5983bc1ab18a54910da83416b3f89f3c7ee43aa	5.5	More Details
CVE-2024-39476	In the Linux kernel, the following vulnerability has been resolved: md/raid5: fix deadlock that raid5d() wait for itself to clear MD_SB_CHANGE_PENDING Xiao reported that lvm2 test lvconvert-raid-takeover.sh can hang with small possibility, the root cause is exactly the same as commit bed9e27baf52 ("Revert "md/raid5: Wait for MD_SB_CHANGE_PENDING in raid5d"") However, Dan reported another hang after that, and junxiao investigated the problem and found out that this is caused by plugged bio can't issue from raid5d(). Current implementation in raid5d() has a weird dependence: 1) md_check_recovery() from raid5d() must hold 'reconfig_mutex' to clear MD_SB_CHANGE_PENDING; 2) raid5d() handles IO in a deadloop, until all IO are issued; 3) IO from raid5d() must wait for MD_SB_CHANGE_PENDING to be cleared; This behaviour is introduce before v2.6, and for consequence, if other context hold 'reconfig_mutex', and md_check_recovery() can't update super_block, then raid5d() will waste one cpu 100% by the deadloop, until 'reconfig_mutex' is released. Refer to the implementation from raid1 and raid10, fix this problem by skipping issue IO if MD_SB_CHANGE_PENDING is still set after md_check_recovery(), daemon thread will be woken up when 'reconfig_mutex' is released. Meanwhile, the hang problem will be fixed as well.	5.5	More Details
CVE-2024-39475	In the Linux kernel, the following vulnerability has been resolved: fbdev: savage: Handle err return when savagefb_check_var failed The commit 04e5eac8f3ab("fbdev: savage: Error out if pixclock equals zero") checks the value of pixclock to avoid divide-by-zero error. However the function savagefb_probe doesn't handle the error return of savagefb_check_var. When pixclock is 0, it will cause divide-by-zero error.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39474	In the Linux kernel, the following vulnerability has been resolved: mm/vmalloc: fix vmalloc which may return null if called with __GFP_NOFAIL commit a421ef303008 ("mm: allow !GFP_KERNEL allocations for kvmalloc") includes support for __GFP_NOFAIL, but it presents a conflict with commit dd544141b9eb ("vmalloc: back off when the current task is OOM-killed"). A possible scenario is as follows: process-a __vmalloc_node_range(GFP_KERNEL | __GFP_NOFAIL) __vmalloc_area_node() vm_area_alloc_pages() --> oom-killer send SIGKILL to process-a if (fatal_signal_pending(current)) break; --> return NULL; To fix this, do not check fatal_signal_pending() in vm_area_alloc_pages() if __GFP_NOFAIL set. This issue occurred during OPLUS KASAN TEST. Below is part of the log -> oom-killer sends signal to process [65731.222840] [T1308] oom-kill:constraint=CONSTRAINT_NONE,nodemask=(null),cpuset=/,mems_allowed=0,global_oom,task_memcg=/apps/uid_10198,task=gs.intelligence,pid=32454,uid=10198 [65731.259685] [T32454] Call trace: [65731.259698] [T32454] dump_backtrace+0xf4/0x118 [65731.259734] [T32454] show_stack+0x18/0x24 [65731.259756] [T32454] dump_stack_lvl+0x60/0x7c [65731.259781] [T32454] dump_stack+0x18/0x38 [65731.259800] [T32454] mrdump_common_die+0x250/0x39c [mrdump] [65731.259936] [T32454] ipanic_die+0x20/0x34 [mrdump] [65731.260019] [T32454] atomic_notifier_call_chain+0xb4/0xfc [65731.260047] [T32454] notify_die+0x114/0x198 [65731.260073] [T32454] die+0xf4/0x5b4 [65731.260098] [T32454] die_kernel_fault+0x80/0x98 [65731.260124] [T32454] __do_kernel_fault+0x160/0x2a8 [65731.260146] [T32454] do_bad_area+0x68/0x148 [65731.260174] [T32454] do_mem_abort+0x151c/0x1b34 [65731.260204] [T32454] el1_abort+0x3c/0x5c [65731.260227] [T32454] el1h_64_sync_handler+0x54/0x90 [65731.260248] [T32454] el1h_64_sync+0x68/0x6c [65731.260269] [T32454] z_erofs_decompress_queue+0x7f0/0x2258 --> be->decompressed_pages = kvcalloc(be->nr_pages, sizeof(struct page *), GFP_KERNEL | __GFP_NOFAIL); kernel panic by NULL pointer dereference. erofs assume kvmalloc with __GFP_NOFAIL never return NULL. [65731.260293] [T32454] z_erofs_runqueue+0xf30/0x104c [65731.260314] [T32454] z_erofs_readahead+0x4f0/0x968 [65731.260339] [T32454] read_pages+0x170/0xadc [65731.260364] [T32454] page_cache_ra_unbounded+0x874/0xf30 [65731.260388] [T32454] page_cache_ra_order+0x24c/0x714 [65731.260411] [T32454] filemap_fault+0xbf0/0x1a74 [65731.260437] [T32454] __do_fault+0xd0/0x33c [65731.260462] [T32454] handle_mm_fault+0xf74/0x3fe0 [65731.260486] [T32454] do_mem_abort+0x54c/0x1b34 [65731.260509] [T32454] el0_da+0x44/0x94 [65731.260531] [T32454] el0t_64_sync_handler+0x98/0xb4 [65731.260553] [T32454] el0t_64_sync+0x198/0x19c	5.5	More Details
CVE-2024-37437	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Elementor Elementor Website Builder allows Cross-Site Scripting (XSS), Stored XSS.This issue affects Elementor Website Builder: from n/a through 3.22.1.	5.5	More Details
CVE-2024-39473	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: ipc4-topology: Fix input format query of process modules without base extension If a process module does not have base config extension then the same format applies to all of it's inputs and the process->base_config_ext is NULL, causing NULL dereference when specifically crafted topology and sequences used.	5.5	More Details
CVE-2024-39472	In the Linux kernel, the following vulnerability has been resolved: xfs: fix log recovery buffer allocation for the legacy h_size fixup Commit a70f9fe52daa ("xfs: detect and handle invalid iclog size set by mkfs") added a fixup for incorrect h_size values used for the initial umount record in old xfsprogs versions. Later commit 0c771b99d6c9 ("xfs: clean up calculation of LR header blocks") cleaned up the log reover buffer calculation, but stoped using the fixed up h_size value to size the log recovery buffer, which can lead to an out of bounds access when the incorrect h_size does not come from the old mkfs tool, but a fuzzer. Fix this by open coding xlog_logrec_hblks and taking the fixed h_size into account for this calculation.	5.5	More Details
CVE-2024-39482	In the Linux kernel, the following vulnerability has been resolved: bcache: fix variable length array abuse in btree_iter btree_iter is used in two ways: either allocated on the stack with a fixed size MAX_BSETS, or from a mempool with a dynamic size based on the specific cache set. Previously, the struct had a fixed-length array of size MAX_BSETS which was indexed out-of-bounds for the dynamically-sized iterators, which causes UBSAN to complain. This patch uses the same approach as in bcachefs's sort_iter and splits the iterator into a btree_iter with a flexible array member and a btree_iter_stack which embeds a btree_iter as well as a fixed-length data array.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39483	In the Linux kernel, the following vulnerability has been resolved: KVM: SVM: WARN on vNMI + NMI window iff NMIs are outright masked When requesting an NMI window, WARN on vNMI support being enabled if and only if NMIs are actually masked, i.e. if the vCPU is already handling an NMI. KVM's ABI for NMIs that arrive simultanesouly (from KVM's point of view) is to inject one NMI and pend the other. When using vNMI, KVM pends the second NMI simply by setting V_NMI_PENDING, and lets the CPU do the rest (hardware automatically sets V_NMI_BLOCKING when an NMI is injected). However, if KVM can't immediately inject an NMI, e.g. because the vCPU is in an STI shadow or is running with GIF=0, then KVM will request an NMI window and trigger the WARN (but still function correctly). Whether or not the GIF=0 case makes sense is debatable, as the intent of KVM's behavior is to provide functionality that is as close to real hardware as possible. E.g. if two NMIs are sent in quick succession, the probability of both NMIs arriving in an STI shadow is infinitesimally low on real hardware, but significantly larger in a virtual environment, e.g. if the vCPU is preempted in the STI shadow. For GIF=0, the argument isn't as clear cut, because the window where two NMIs can collide is much larger in bare metal (though still small). That said, KVM should not have divergent behavior for the GIF=0 case based on whether or not vNMI support is enabled. And KVM has allowed simultaneous NMIs with GIF=0 for over a decade, since commit 7460fb4a3400 ("KVM: Fix simultaneous NMIs"). I.e. KVM's GIF=0 handling shouldn't be modified without a *really* good reason to do so, and if KVM's behavior were to be modified, it should be done irrespective of vNMI support.	5.5	More Details
CVE-2024-39484	In the Linux kernel, the following vulnerability has been resolved: mmc: davinci: Don't strip remove function when driver is builtin Using __exit for the remove function results in the remove callback being discarded with CONFIG_MMC_DAVINCI=y. When such a device gets unbound (e.g. using sysfs or hotplug), the driver is just removed without the cleanup being performed. This results in resource leaks. Fix it by compiling in the remove callback unconditionally. This also fixes a W=1 modpost warning: WARNING: modpost: drivers/mmc/host/davinci_mmc: section mismatch in reference: davinci_mmcsd_driver+0x10 (section: .data) -> davinci_mmcsd_remove (section: .exit.text)	5.5	More Details
CVE-2024-39485	In the Linux kernel, the following vulnerability has been resolved: media: v4l: async: Properly re-initialise notifier entry in unregister The notifier_entry of a notifier is not re-initialised after unregistering the notifier. This leads to dangling pointers being left there so use list_del_init() to return the notifier_entry an empty list.	5.5	More Details
CVE-2023-39328	A vulnerability was found in OpenJPEG similar to CVE-2019-6988. This flaw allows an attacker to bypass existing protections and cause an application crash through a maliciously crafted file.	5.5	More Details
CVE-2024-39478	In the Linux kernel, the following vulnerability has been resolved: crypto: starfive - Do not free stack buffer RSA text data uses variable length buffer allocated in software stack. Calling kfree on it causes undefined behaviour in subsequent operations.	5.5	More Details
CVE-2024-39072	AMTT Hotel Broadband Operation System (HiBOS) v3.0.3.151204 is vulnerable to SQL injection via manager/conference/calendar_remind.php.	5.5	More Details
CVE-2024-6613	The frame iterator could get stuck in a loop when encountering certain wasm frames leading to incorrect stack traces. This vulnerability affects Firefox < 128 and Thunderbird < 128.	5.5	More Details
CVE-2024-37172	SAP S/4HANA Finance (Advanced Payment Management) does not perform necessary authorization check for an authenticated user, resulting in escalation of privileges. As a result, it has a low impact to confidentiality and availability but there is no impact on the integrity.	5.4	More Details
CVE-2024-5600	The SCSS Happy Compiler – Compile SCSS to CSS & Automatic Enqueue plugin for WordPress is vulnerable to Stored Cross-Site Scripting due to a missing capability check and insufficient sanitization on the import_settings() function in all versions up to, and including, 1.3.10. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject malicious web scripts.	5.4	More Details
CVE-2024-39308	RailsAdmin is a Rails engine that provides an interface for managing data. RailsAdmin list view has the XSS vulnerability, caused by improperly-escaped HTML title attribute. Upgrade to 3.1.3 or 2.2.2 (to be released).	5.4	More Details
CVE-2024-6229	A stored cross-site scripting (XSS) vulnerability exists in the 'Upload Knowledge' feature of stangirard/quivr, affecting the latest version. Users can upload files via URL, which allows the insertion of malicious JavaScript payloads. These payloads are stored on the server and executed whenever any user clicks on a link containing the payload, leading to potential data theft, session hijacking, and reputation damage.	5.4	More Details
CVE-2024-37542	Missing Authorization vulnerability in WpDevArt Responsive Image Gallery, Gallery Album.This issue affects Responsive Image Gallery, Gallery Album: from n/a through 2.0.3.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39021	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/vpsApiData_deal.php?mudi=del	5.4	More Details
CVE-2024-4102	The Pricing Table plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the ajax() function in all versions up to, and including, 2.0.1. This makes it possible for authenticated attackers, with subscriber-level access and above, to perform unauthorized actions like editing pricing tables.	5.4	More Details
CVE-2024-39031	In Silverpeas Core <= 6.3.5, in Mes Agendas, a user can create new events and add them to their calendar. Additionally, users can invite others from the same domain, including administrators, to these events. A standard user can inject an XSS payload into the "Titre" and "Description" fields when creating an event and then add the administrator or any user to the event. When the invited user (victim) views their own profile, the payload will be executed on their side, even if they do not click on the event.	5.4	More Details
CVE-2024-5648	The LearnDash LMS – Reports plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several functions in all versions up to, and including, 1.8.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update various plugin settings.	5.4	More Details
CVE-2024-39019	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/idcProData_deal.php?mudi=del	5.4	More Details
CVE-2024-37502	Deserialization of Untrusted Data vulnerability in wpweb WooCommerce Social Login.This issue affects WooCommerce Social Login: from n/a through 2.6.3.	5.4	More Details
CVE-2024-37923	Cross-Site Request Forgery (CSRF) vulnerability in Cliengo – Chatbot.This issue affects Cliengo – Chatbot: from n/a through 3.0.1.	5.4	More Details
CVE-2024-39178	MyPower vc8100 V100R001C00B030 was discovered to contain an arbitrary file read vulnerability via the component /tcpdump/tcpdump.php?menu_uuid.	5.4	More Details
CVE-2024-27716	Cross Site Scripting vulnerability in Eskooly Web Product v.3.0 and before allows a remote attacker to execute arbitrary code via the message sending and user input fields.	5.4	More Details
CVE-2024-29318	Volmarg Personal Management System 1.4.64 is vulnerable to stored cross site scripting (XSS) via upload of a SVG file with embedded javascript code.	5.4	More Details
CVE-2024-39595	SAP Business Warehouse - Business Planning and Simulation application does not sufficiently encode user-controlled inputs, resulting in Stored Cross-Site Scripting (XSS) vulnerability. This vulnerability allows users to modify website content and on successful exploitation, an attacker can cause low impact to the confidentiality and integrity of the application.	5.4	More Details
CVE-2024-38971	vaeThink 1.0.2 is vulnerable to stored Cross Site Scripting (XSS) in the system backend.	5.4	More Details
CVE-2024-39929	Exim through 4.97.1 misparses a multiline RFC 2231 header filename, and thus remote attackers can bypass a $mime_filename extension-blocking protection mechanism, and potentially deliver executable attachments to the mailboxes of end users.	5.4	More Details
CVE-2024-38344	A cross-site request forgery vulnerability exists in WP Tweet Walls versions prior to 1.0.4. If this vulnerability is exploited, an attacker allows a user who logs in to the WordPress site where the affected plugin is enabled to access a malicious page. As a result, the user may perform unintended operations on the WordPress site.	5.4	More Details
CVE-2024-5993	The Cliengo – Chatbot plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_session' function in all versions up to, and including, 3.0.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the session token of the chatbot.	5.4	More Details
CVE-2024-21730	The fancyselect list field layout does not correctly escape inputs, leading to a self-XSS vector.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39900	OpenSearch Dashboards Reports allows ‘Report Owner’ export and share reports from OpenSearch Dashboards. An issue in the OpenSearch reporting plugin allows unintended access to private tenant resources like notebooks. The system did not properly check if the user was the resource author when accessing resources in a private tenant, leading to potential data being revealed. The patches are included in OpenSearch 2.14.	5.4	More Details
CVE-2024-2234	The Himer WordPress theme before 2.1.1 does not sanitise and escape some of its Post settings, which could allow high privilege users such as Contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2024-37934	Improper Control of Generation of Code ('Code Injection') vulnerability in Saturday Drive Ninja Forms allows Code Injection.This issue affects Ninja Forms: from n/a through 3.8.4.	5.4	More Details
CVE-2024-39248	A cross-site scripting (XSS) vulnerability in SimpCMS v0.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title field at /admin.php.	5.4	More Details
CVE-2024-27785	An improper neutralization of formula elements in a CSV File vulnerability [CWE-1236] in FortiAIOps version 2.0.0 may allow a remote authenticated attacker to execute arbitrary commands on a client's workstation via poisoned CSV reports.	5.4	More Details
CVE-2024-29507	Artifex Ghostscript before 10.03.0 sometimes has a stack-based buffer overflow via the CIDFSubstPath and CIDFSubstFont parameters.	5.4	More Details
CVE-2024-2375	The WPQA Builder WordPress plugin before 6.1.1 does not sanitise and escape some of its Slider settings, which could allow high privilege users such as contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2024-22377	The deploy directory in PingFederate runtime nodes is reachable to unauthorized users.	5.3	More Details
CVE-2024-31223	Fides is an open-source privacy engineering platform, and `SERVER_SIDE_FIDES_API_URL` is a server-side configuration environment variable used by the Fides Privacy Center to communicate with the Fides webserver backend. The value of this variable is a URL which typically includes a private IP address, private domain name, and/or port. A vulnerability present starting in version 2.19.0 and prior to version 2.39.2rc0 allows an unauthenticated attacker to make a HTTP GET request from the Privacy Center that discloses the value of this server-side URL. This could result in disclosure of server-side configuration giving an attacker information on server-side ports, private IP addresses, and/or private domain names. The vulnerability has been patched in Fides version 2.39.2rc0. No known workarounds are available.	5.3	More Details
CVE-2024-6428	Mattermost versions 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2, 9.5.x <= 9.5.5 fail to prevent specifying a RemoteId when creating a new user which allows an attacker to specify both a remoteId and the user ID, resulting in creating a user with a user-defined user ID. This can cause some broken functionality in User Management such administrative actions against the user not working.	5.3	More Details
CVE-2024-23588	HCL Nomad server on Domino fails to properly handle users configured with limited Domino access resulting in a possible denial of service vulnerability.	5.3	More Details
CVE-2024-3653	A vulnerability was found in Undertow. This issue requires enabling the learning-push handler in the server's config, which is disabled by default, leaving the maxAge config in the handler unconfigured. The default is -1, which makes the handler vulnerable. If someone overwrites that config, the server is not subject to the attack. The attacker needs to be able to reach the server with a normal HTTP request.	5.3	More Details
CVE-2024-39312	Botan is a C++ cryptography library. X.509 certificates can identify elliptic curves using either an object identifier or using explicit encoding of the parameters. A bug in the parsing of name constraint extensions in X.509 certificates meant that if the extension included both permitted subtrees and excluded subtrees, only the permitted subtree would be checked. If a certificate included a name which was permitted by the permitted subtree but also excluded by excluded subtree, it would be accepted. Fixed in versions 3.5.0 and 2.19.5.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34702	Botan is a C++ cryptography library. X.509 certificates can identify elliptic curves using either an object identifier or using explicit encoding of the parameters. Prior to 3.5.0 and 2.19.5, checking name constraints in X.509 certificates is quadratic in the number of names and name constraints. An attacker who presented a certificate chain which contained a very large number of names in the SubjectAlternativeName, signed by a CA certificate which contained a large number of name constraints, could cause a denial of service. The problem has been addressed in Botan 3.5.0 and a partial backport has also been applied and is included in Botan 2.19.5.	5.3	More Details
CVE-2024-39695	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 v0.28.2. The vulnerability is in the parser for the ASF video format, which was a new feature in v0.28.0. The out-of-bounds read is triggered when Exiv2 is used to read the metadata of a crafted video file. The bug is fixed in version v0.28.3.	5.3	More Details
CVE-2024-23562	A security vulnerability in HCL Domino could allow disclosure of sensitive configuration information. A remote unauthenticated attacker could exploit this vulnerability to obtain information to launch further attacks against the affected system.	5.3	More Details
CVE-2024-6163	Certain http endpoints of Checkmk in Checkmk < 2.3.0p10 < 2.2.0p31, < 2.1.0p46, <= 2.0.0p39 allows remote attacker to bypass authentication and access data	5.3	More Details
CVE-2024-6612	CSP violations generated links in the console tab of the developer tools, pointing to the violating resource. This caused a DNS prefetch which leaked that a CSP violation happened. This vulnerability affects Firefox < 128 and Thunderbird < 128.	5.3	More Details
CVE-2024-35270	Windows iSCSI Service Denial of Service Vulnerability	5.3	More Details
CVE-2024-39899	PrivateBin is an online pastebin where the server has zero knowledge of pasted data. In v1.5, PrivateBin introduced the YOURLS server-side proxy. The idea was to allow using the YOURLs URL shortener without running the YOURLs instance without authentication and/or exposing the authentication token to the public, allowing anyone to shorten any URL. With the proxy mechanism, anyone can shorten any URL pointing to the configured PrivateBin instance. The vulnerability allowed other URLs to be shortened, as long as they contain the PrivateBin instance, defeating the limit imposed by the proxy. This vulnerability is fixed in 1.7.4.	5.3	More Details
CVE-2024-33869	An issue was discovered in Artifex Ghostscript before 10.03.1. Path traversal and command execution can occur (via a crafted PostScript document) because of path reduction in base/gpmisc.c. For example, restrictions on use of %pipe% can be bypassed via the aa/../%pipe%command# output filename.	5.3	More Details
CVE-2024-5810	The WP2Speed Faster – Optimize PageSpeed Insights Score 90-100 plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 1.0.1. This is due to the use of hardcoded credentials to authenticate all the incoming API requests. This makes it possible for unauthenticated attackers to overwrite CSS, update the trial settings, purge the cache, and find attachments.	5.3	More Details
CVE-2024-40038	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/userScore_deal.php?mudi=rev	5.3	More Details
CVE-2024-6383	The bson_string_append function in MongoDB C Driver may be vulnerable to a buffer overflow where the function might attempt to allocate too small of buffer and may lead to memory corruption of neighbouring heap memory. This issue affects libbson versions prior to 1.27.1	5.3	More Details
CVE-2024-6171	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to IP Address Spoofing in all versions up to, and including, 1.5.112 due to insufficient IP address validation and/or use of user-supplied HTTP headers as a primary method for IP retrieval. This makes it possible for unauthenticated attackers to bypass antispam functionality in the Form Builder widgets.	5.3	More Details
CVE-2024-39211	Kaiten 57.128.8 allows remote attackers to enumerate user accounts via a crafted POST request, because a login response contains a user_email field only if the user account exists.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52891	A vulnerability has been identified in SIMATIC Energy Manager Basic (All versions < V7.5), SIMATIC Energy Manager PRO (All versions < V7.5), SIMATIC IPC DiagBase (All versions), SIMATIC IPC DiagMonitor (All versions), SIMIT V10 (All versions), SIMIT V11 (All versions < V11.1). Unified Automation .NET based OPC UA Server SDK before 3.2.2 used in Siemens products are affected by a similar vulnerability as documented in CVE-2023-27321 for the OPC Foundation UA .NET Standard implementation. A successful attack may lead to high load situation and memory exhaustion, and may block the server.	5.3	More Details
CVE-2024-40750	Linksys Velop Pro 6E 1.0.8 MX6200_1.0.8.215731 and 7 1.0.10.215314 devices send cleartext Wi-Fi passwords over the public Internet during app-based installation.	5.3	More Details
CVE-2024-3228	The Social Sharing Plugin – Kiwi plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 2.1.7 via the 'kiwi-nw-pinterest' class. This makes it possible for unauthenticated attackers to view limited content from password protected posts.	5.3	More Details
CVE-2024-3608	The Product Designer plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the product_designer_ajax_delete_attach_id() function in all versions up to, and including, 1.0.33. This makes it possible for unauthenticated attackers to delete arbitrary attachments.	5.3	More Details
CVE-2024-4100	The Pricing Table plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.1. This is due to missing or incorrect nonce validation on the ajax() function. This makes it possible for unauthenticated attackers to perform a variety of actions related to managing pricing tables via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.3	More Details
CVE-2024-37430	Authentication Bypass by Spoofing vulnerability in Patreon Patreon WordPress allows Functionality Misuse.This issue affects Patreon WordPress: from n/a through 1.9.0.	5.3	More Details
CVE-2024-28068	A vulnerability was discovered in SS in Samsung Mobile Processor, Wearable Processor, and Modems with versions Exynos 9820, Exynos 9825, Exynos 980, Exynos 990, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 2400, Exynos 9110, Exynos W920, Exynos W930, Exynos Modem 5123, and Exynos Modem 5300 that involves a NULL pointer dereference which can cause abnormal termination of a mobile phone via a manipulated packet.	5.3	More Details
CVE-2024-28067	A vulnerability in Samsung Exynos Modem 5300 allows a Man-in-the-Middle (MITM) attacker to downgrade the security mode of packets going to the victim, enabling the attacker to send messages to the victim in plaintext.	5.3	More Details
CVE-2024-27361	A vulnerability was discovered in Samsung Mobile Processor Exynos 980, Exynos 990, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, and Exynos 2400 that involves a time-of-check to time-of-use (TOCTOU) race condition, which can lead to a Denial of Service.	5.1	More Details
CVE-2023-3290	A BOLA vulnerability in POST /customers allows a low privileged user to create a low privileged user (customer) in the system. This results in unauthorized data manipulation.	5.0	More Details
CVE-2024-39600	Under certain conditions, the memory of SAP GUI for Windows contains the password used to log on to an SAP system, which might allow an attacker to get hold of the password and impersonate the affected user. As a result, it has a high impact on the confidentiality but there is no impact on the integrity and availability.	5.0	More Details
CVE-2024-37171	SAP Transportation Management (Collaboration Portal) allows an attacker with non-administrative privileges to send a crafted request from a vulnerable web application. This will trigger the application handler to send a request to an unintended service, which may reveal information about that service. The information obtained could be used to target internal systems behind firewalls that are normally inaccessible to an attacker from the external network, resulting in a Server-Side Request Forgery vulnerability. There is no effect on integrity or availability of the application.	5.0	More Details
CVE-2024-34689	WebFlow Services of SAP Business Workflow allows an authenticated attacker to enumerate accessible HTTP endpoints in the internal network by specially crafting HTTP requests. On successful exploitation this can result in information disclosure. It has no impact on integrity and availability of the application.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39699	Directus is a real-time API and App dashboard for managing SQL database content. There was already a reported SSRF vulnerability via file import. It was fixed by resolving all DNS names and checking if the requested IP is an internal IP address. However it is possible to bypass this security measure and execute a SSRF using redirects. Directus allows redirects when importing file from the URL and does not check the result URL. Thus, it is possible to execute a request to an internal IP, for example to 127.0.0.1. However, it is blind SSRF, because Directus also uses response interception technique to get the information about the connect from the socket directly and it does not show a response if the IP address is internal. This vulnerability is fixed in 10.9.3.	5.0	More Details
CVE-2024-39598	SAP CRM (WebClient UI Framework) allows an authenticated attacker to enumerate accessible HTTP endpoints in the internal network by specially crafting HTTP requests. On successful exploitation this can result in information disclosure. It has no impact on integrity and availability of the application.	5.0	More Details
CVE-2024-37208	Server-Side Request Forgery (SSRF) vulnerability in Robert Macchi WP Scraper.This issue affects WP Scraper: from n/a through 5.7.	4.9	More Details
CVE-2024-38970	vaeThink 1.0.2 is vulnerable to Information Disclosure via the system backend,access management administrator function.	4.9	More Details
CVE-2024-37266	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Themeum Tutor LMS allows Path Traversal.This issue affects Tutor LMS: from n/a through 2.7.1.	4.9	More Details
CVE-2024-37410	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Beaver Addons PowerPack Lite for Beaver Builder allows Path Traversal.This issue affects PowerPack Lite for Beaver Builder: from n/a through 1.3.0.3.	4.9	More Details
CVE-2024-37464	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WPZOOM Beaver Builder Addons by WPZOOM allows Path Traversal.This issue affects Beaver Builder Addons by WPZOOM: from n/a through 1.3.5.	4.9	More Details
CVE-2024-36113	Discourse is an open-source discussion platform. Prior to version 3.2.3 on the `stable` branch, version 3.3.0.beta3 on the `beta` branch, and version 3.3.0.beta4-dev on the `tests-passed` branch, a rogue staff user could suspend other staff users preventing them from logging in to the site. The issue is patched in version 3.2.3 on the `stable` branch, version 3.3.0.beta3 on the `beta` branch, and version 3.3.0.beta4-dev on the `tests-passed` branch. No known workarounds are available.	4.9	More Details
CVE-2023-50181	An improper access control vulnerability [CWE-284] in Fortinet FortiADC version 7.4.0 through 7.4.1 and before 7.2.4 allows a read only authenticated attacker to perform some write actions via crafted HTTP or HTTPS requests.	4.9	More Details
CVE-2024-40599	An issue was discovered in the GuMaxDD skin for MediaWiki through 1.42.1. There is stored XSS via MediaWiki:Sidebar top-level menu entries.	4.8	More Details
CVE-2023-50179	An improper certificate validation vulnerability [CWE-295] in FortiADC 7.4.0, 7.2 all versions, 7.1 all versions, 7.0 all versions may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and public SDN connectors.	4.8	More Details
CVE-2024-5802	The URL Shortener by Myhop WordPress plugin through 1.0.17 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-2024-40600	An issue was discovered in the Metrolook skin for MediaWiki through 1.42.1. There is stored XSS via MediaWiki:Sidebar top-level menu entries.	4.8	More Details
CVE-2024-40604	An issue was discovered in the Nimbus skin for MediaWiki through 1.42.1. There is Stored XSS via MediaWiki:Nimbus-sidebar menu and submenu entries.	4.8	More Details
CVE-2024-40602	An issue was discovered in the Tempo skin for MediaWiki through 1.42.1. There is stored XSS via MediaWiki:Sidebar top-level menu entries.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33509	An improper certificate validation vulnerability [CWE-295] in FortiWeb 7.2.0 through 7.2.1, 7.0 all versions, 6.4 all versions and 6.3 all versions may allow a remote and unauthenticated attacker in a Man-in-the-Middle position to decipher and/or tamper with the communication channel between the device and different endpoints used to fetch data for Web Application Firewall (WAF).	4.8	More Details
CVE-2024-37528	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 294293.	4.8	More Details
CVE-2024-40605	An issue was discovered in the Foreground skin for MediaWiki through 1.42.1. There is stored XSS via MediaWiki:Sidebar top-level menu entries.	4.8	More Details
CVE-2024-39599	Due to a Protection Mechanism Failure in SAP NetWeaver Application Server for ABAP and ABAP Platform, a developer can bypass the configured malware scanner API because of a programming error. This leads to a low impact on the application's confidentiality, integrity, and availability.	4.7	More Details
CVE-2024-30071	Windows Remote Access Connection Manager Information Disclosure Vulnerability	4.7	More Details
CVE-2024-6601	A race condition could lead to a cross-origin container obtaining permissions of the top-level origin. This vulnerability affects Firefox < 128, Firefox ESR < 115.13, Thunderbird < 115.13, and Thunderbird < 128.	4.7	More Details
CVE-2024-39723	IBM FlashSystem 5300 USB ports may be usable even if the port has been disabled by the administrator. A user with physical access to the system could use the USB port to cause loss of access to data. IBM X-Force ID: 295935.	4.6	More Details
CVE-2024-37389	Apache NiFi 1.10.0 through 1.26.0 and 2.0.0-M1 through 2.0.0-M3 support a description field in the Parameter Context configuration that is vulnerable to cross-site scripting. An authenticated user, authorized to configure a Parameter Context, can enter arbitrary JavaScript code, which the client browser will execute within the session context of the authenticated user. Upgrading to Apache NiFi 1.27.0 or 2.0.0-M4 is the recommended mitigation.	4.6	More Details
CVE-2024-27362	A vulnerability was discovered in Samsung Mobile Processors Exynos 1280, Exynos 2200, Exynos 1330, Exynos 1380, and Exynos 2400 where they do not properly check the length of the data, which can lead to a Information disclosure.	4.4	More Details
CVE-2024-6608	It was possible to move the cursor using pointerlock from an iframe. This allowed moving the cursor outside of the viewport and the Firefox window. This vulnerability affects Firefox < 128 and Thunderbird < 128.	4.3	More Details
CVE-2024-6610	Form validation popups could capture escape key presses. Therefore, spamming form validation messages could be used to prevent users from exiting full-screen mode. This vulnerability affects Firefox < 128 and Thunderbird < 128.	4.3	More Details
CVE-2024-2233	The Himer WordPress theme before 2.1.1 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks. These include declining and accepting group invitations or leaving a group	4.3	More Details
CVE-2024-2235	The Himer WordPress theme before 2.1.1 does not have CSRF checks in some places, which could allow attackers to make users vote on any polls, including those they don't have access to via a CSRF attack	4.3	More Details
CVE-2024-39875	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application allows authenticated, low privilege users with the 'Manage own remote connections' permission to retrieve details about other users and group memberships.	4.3	More Details
CVE-2024-6614	The frame iterator could get stuck in a loop when encountering certain wasm frames leading to incorrect stack traces. This vulnerability affects Firefox < 128 and Thunderbird < 128.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52238	A vulnerability has been identified in RUGGEDCOM RST2228 (All versions < V5.9.0), RUGGEDCOM RST2228P (All versions < V5.9.0). The web server of the affected systems leaks the MACSEC key in clear text to a logged in user. An attacker with the credentials of a low privileged user could retrieve the MACSEC key and access (decrypt) the ethernet frames sent by authorized recipients.	4.3	More Details
CVE-2024-39920	The TCP protocol in RFC 9293 has a timing side channel that makes it easier for remote attackers to infer the content of one TCP connection from a client system (to any server), when that client system is concurrently obtaining TCP data at a slow rate from an attacker-controlled server, aka the "SnailLoad" issue. For example, the attack can begin by measuring RTTs via the TCP segments whose role is to provide an ACK control bit and an Acknowledgment Number.	4.3	More Details
CVE-2024-5856	The Comment Images Reloaded plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the cir_delete_image AJAX action in all versions up to, and including, 2.2.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary media attachments.	4.3	More Details
CVE-2024-2040	The Himer WordPress theme before 2.1.1 does not have CSRF checks in some places, which could allow attackers to make users join private groups via a CSRF attack	4.3	More Details
CVE-2024-4543	The Snippet Shortcodes plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.1.4. This is due to missing or incorrect nonce validation when adding or editing shortcodes. This makes it possible for unauthenticated attackers to modify shortcodes via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-21759	An authorization bypass through user-controlled key in Fortinet FortiPortal version 7.2.0, and versions 7.0.0 through 7.0.6 allows attacker to view unauthorized resources via HTTP or HTTPS requests.	4.3	More Details
CVE-2024-6167	The Just Custom Fields plugin for WordPress is vulnerable to unauthorized access of functionality due to a missing capability check on several AJAX functions in all versions up to, and including, 3.3.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to invoke this functionality intended for admin users. This enables subscribers to manage field groups, change visibility of items among other things.	4.3	More Details
CVE-2024-6168	The Just Custom Fields plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.3.2. This is due to missing or incorrect nonce validation on several AJAX function. This makes it possible for unauthenticated attackers to invoke this functionality intended for admin users via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This enables subscribers to manage field groups, change visibility of items among other things.	4.3	More Details
CVE-2024-5704	The XPlainer – WooCommerce Product FAQ [WooCommerce Accordion FAQ Plugin plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several functions in all versions up to, and including, 1.6.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to add new and update existing FAQs, FAQ lists, and modify FAQ associations with products.	4.3	More Details
CVE-2024-37175	SAP CRM WebClient does not perform necessary authorization check for an authenticated user, resulting in escalation of privileges. This could allow an attacker to access some sensitive information.	4.3	More Details
CVE-2024-40603	An issue was discovered in the ArticleRatings extension for MediaWiki through 1.42.1. Special:ChangeRating allows CSRF to alter data via a GET request.	4.3	More Details
CVE-2024-40598	An issue was discovered in the CheckUser extension for MediaWiki through 1.42.1. The API can expose suppressed information for log events. (The log_deleted attribute is not applied to entries.)	4.3	More Details
CVE-2024-40596	An issue was discovered in the CheckUser extension for MediaWiki through 1.42.1. The Special:Investigate feature can expose suppressed information for log events. (TimelineService does not support properly suppressing.)	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39691	matrix-appservice-irc is a Node.js IRC bridge for the Matrix messaging protocol. The fix for GHSA-wm4w-7h2q-3pf7 / CVE-2024-32000 included in matrix-appservice-irc 2.0.0 relied on the Matrix homeserver-provided timestamp to determine whether a user has access to the event they're replying to when determining whether or not to include a truncated version of the original event in the IRC message. Since this value is controlled by external entities, a malicious Matrix homeserver joined to a room in which a matrix-appservice-irc bridge instance (before version 2.0.1) is present can fabricate the timestamp with the intent of tricking the bridge into leaking room messages the homeserver should not have access to. matrix-appservice-irc 2.0.1 drops the reliance on `origin_server_ts` when determining whether or not an event should be visible to a user, instead tracking the event timestamps internally. As a workaround, it's possible to limit the amount of information leaked by setting a reply template that doesn't contain the original message.	4.3	More Details
CVE-2024-28882	OpenVPN from 2.6.0 through 2.6.10 in a server role accepts multiple exit notifications from authenticated clients which will extend the validity of a closing session	4.3	More Details
CVE-2024-3410	The DN Footer Contacts WordPress plugin before 1.6.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.3	More Details
CVE-2024-5855	The Media Hygiene: Remove or Delete Unused Images and More! plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the bulk_action_delete and delete_single_image_call AJAX actions in all versions up to, and including, 3.0.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary attachments. A nonce check was added in version 3.0.1, however, it wasn't until version 3.0.2 that a capability check was added.	4.3	More Details
CVE-2024-39897	zot is an OCI image registry. Prior to 2.1.0, the cache driver `GetBlob()` allows read access to any blob without access control check. If a Zot `accessControl` policy allows users read access to some repositories but restricts read access to other repositories and `dedupe` is enabled (it is enabled by default), then an attacker who knows the name of an image and the digest of a blob (that they do not have read access to), they may maliciously read it via a second repository they do have read access to. This attack is possible because [`ImageStore.CheckBlob()` calls `checkCacheBlob()`] (https://github.com/project-zot/zot/blob/v2.1.0-rc2/pkg/storage/imagestore/imagestore.go#L1158-L1159) to find the blob a global cache by searching for the digest. If it is found, it is copied to the user requested repository with `copyBlob()`. The attack may be mitigated by configuring "dedupe": false in the "storage" settings. The vulnerability is fixed in 2.1.0.	4.3	More Details
CVE-2024-31897	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 288178.	4.3	More Details
CVE-2024-39596	Due to missing authorization checks, SAP Enable Now allows an author to escalate privileges to access information which should otherwise be restricted. On successful exploitation, the attacker can cause limited impact on confidentiality of the application.	4.3	More Details
CVE-2024-35234	Discourse is an open-source discussion platform. Prior to version 3.2.3 on the `stable` branch and version 3.3.0.beta3 on the `tests-passed` branch, an attacker can execute arbitrary JavaScript on users' browsers by posting a specific URL containing maliciously crafted meta tags. This issue only affects sites with Content Security Polic (CSP) disabled. The problem has been patched in version 3.2.3 on the `stable` branch and version 3.3.0.beta3 on the `tests-passed` branch. As a workaround, ensure CSP is enabled on the forum.	4.2	More Details
CVE-2024-39901	OpenSearch Observability is collection of plugins and applications that visualize data-driven events. An issue in the OpenSearch observability plugins allows unintended access to private tenant resources like notebooks. The system did not properly check if the user was the resource author when accessing resources in a private tenant, leading to potential data being revealed. The patches are included in OpenSearch 2.14.	4.2	More Details
CVE-2024-37180	Under certain conditions SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker to access remote-enabled function module with no further authorization which would otherwise be restricted, the function can be used to read non-sensitive information with low impact on confidentiality of the application.	4.1	More Details
CVE-2024-34603	Improper access control in Samsung Message prior to SMR Jul-2024 Release 1 allows local attackers to access location data.	4.0	More Details
CVE-2024-39876	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected applications do not properly handle log rotation. This could allow an unauthenticated remote attacker to cause a denial of service condition through resource exhaustion on the device.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37442	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Photo Gallery Team Photo Gallery by Ays allows Code Injection.This issue affects Photo Gallery by Ays: from n/a before 5.7.1.	3.8	More Details
CVE-2024-37234	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Kodezen Limited Academy LMS.This issue affects Academy LMS: from n/a through 2.0.4.	3.5	More Details
CVE-2024-6539	A vulnerability classified as problematic has been found in heyewei SpringBootCMS up to 2024-05-28. Affected is an unknown function of the file /guestbook of the component Guestbook Handler. The manipulation of the argument Content leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-270450 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-6526	A vulnerability classified as problematic has been found in CodeIgniter Ecommerce-CodeIgniter-Bootstrap up to 1998845073cf433bc6c250b0354461fbd84d0e03. This affects an unknown part. The manipulation of the argument search_title/catName/sub/name/categorie leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 1b3da45308bb6c3f55247d0e99620b600bd85277. It is recommended to apply a patch to fix this issue. The identifier VDB-270369 was assigned to this vulnerability.	3.5	More Details
CVE-2024-35777	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Automattic WooCommerce allows Content Spoofing.This issue affects WooCommerce: from n/a through 8.9.2.	3.5	More Details
CVE-2024-6523	A vulnerability was found in ZKTeco BioTime up to 9.5.2. It has been classified as problematic. Affected is an unknown function of the component system-group-add Handler. The manipulation of the argument user with the input <script>alert('XSS')</script> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-270366 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-21832	A potential JSON injection attack vector exists in PingFederate REST API data stores using the POST method and a JSON request body.	3.5	More Details
CVE-2024-6511	A vulnerability classified as problematic was found in y_project RuoYi up to 4.7.9. Affected by this vulnerability is the function isJsonRequest of the component Content-Type Handler. The manipulation of the argument HttpHeaders.CONTENT_TYPE leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-270343.	3.5	More Details
CVE-2024-26015	An incorrect parsing of numbers with different radices vulnerability [CWE-1389] in FortiProxy version 7.4.3 and below, version 7.2.10 and below, version 7.0.17 and below and FortiOS version 7.4.3 and below, version 7.2.8 and below, version 7.0.15 and below IP address validation feature may permit an unauthenticated attacker to bypass the IP blocklist via crafted requests.	3.4	More Details
CVE-2024-34602	Use of implicit intent for sensitive communication in Samsung Messages prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. User interaction is required for triggering this vulnerability.	3.3	More Details
CVE-2024-29508	Artifex Ghostscript before 10.03.0 has a heap-based pointer disclosure (observable in a constructed BaseFont name) in the function pdf_base_font_alloc.	3.3	More Details
CVE-2024-37996	A vulnerability has been identified in JT Open (All versions < V11.5), JT2Go (All versions < V2406.0003), PLM XML SDK (All versions < V7.1.0.014), Teamcenter Visualization V14.2 (All versions < V14.2.0.13), Teamcenter Visualization V14.3 (All versions < V14.3.0.11), Teamcenter Visualization V2312 (All versions < V2312.0008), Teamcenter Visualization V2406 (All versions < V2406.0003). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted XML files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	3.3	More Details
CVE-2024-34692	Due to missing verification of file type or content, SAP Enable Now allows an authenticated attacker to upload arbitrary files. These files include executables which might be downloaded and executed by the user which could host malware. On successful exploitation an attacker can cause limited impact on confidentiality and Integrity of the application.	3.3	More Details
CVE-2024-6126	A flaw was found in the cockpit package. This flaw allows an authenticated user to kill any process when enabling the pam_env's user_readenv option, which leads to a denial of service (DoS) attack.	3.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6501	A flaw was found in NetworkManager. When a system running NetworkManager with DEBUG logs enabled and an interface eth1 configured with LLDP enabled, a malicious user could inject a malformed LLDP packet. NetworkManager would crash, leading to a denial of service.	3.1	More Details
CVE-2024-32754	Under certain circumstances, when the controller is in factory reset mode waiting for initial setup, it will broadcast its MAC address, serial number, and firmware version. Once configured, the controller will no longer broadcast this information.	3.1	More Details
CVE-2024-6434	The Premium Addons for Elementor plugin for WordPress is vulnerable to Regular Expression Denial of Service (ReDoS) in all versions up to, and including, 4.10.35. This is due to processing user-supplied input as a regular expression. This makes it possible for authenticated attackers, with Author-level access and above, to create and query a malicious post title, resulting in slowing server resources.	3.1	More Details
CVE-2024-39807	Mattermost versions 9.5.x <= 9.5.5 and 9.8.0 fail to properly sanitize the recipients of a webhook event which allows an attacker monitoring webhook events to retrieve the channel IDs of archived or restored channels.	3.1	More Details
CVE-2024-39361	Mattermost versions 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2 and 9.5.x <= 9.5.5 fail to prevent users from specifying a RemoteId for their posts which allows an attacker to specify both a remoteId and the post ID, resulting in creating a post with a user-defined post ID. This can cause some broken functionality in the channel or thread with user-defined posts	3.1	More Details
CVE-2024-6525	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DAR-7000 up to 20230922. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /log/decodmail.php. The manipulation of the argument file leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-270368. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2.7	More Details
CVE-2024-39353	Mattermost versions 9.5.x <= 9.5.5 and 9.8.0 fail to sanitize the RemoteClusterFrame payloads before audit logging them which allows a high privileged attacker with access to the audit logs to read message contents.	2.7	More Details
CVE-2024-36257	Mattermost versions 9.5.x <= 9.5.5 and 9.8.0, when using shared channels with multiple remote servers connected, fail to check that the remote server A requesting the server B to update the profile picture of a user is the remote that actually has the user as a local one . This allows a malicious remote A to change the profile images of users that belong to another remote server C that is connected to the server A.	2.7	More Details
CVE-2024-37253	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in WpDirectoryKit WP Directory Kit allows Code Injection.This issue affects WP Directory Kit: from n/a through 1.3.6.	2.7	More Details
CVE-2024-6469	A vulnerability was found in playSMS 1.4.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /index.php?app=main&inc=feature_firewall&op=firewall_list of the component Template Handler. The manipulation of the argument IP address with the input {{`id`} leads to injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-270277 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.7	More Details
CVE-2024-6470	A vulnerability was found in playSMS 1.4.3. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /index.php?app=main&inc=feature_inboxgroup&op=list of the component Template Handler. The manipulation of the argument Receiver Number with the input {{`id`}} leads to injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-270278 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.7	More Details
CVE-2024-36122	Discourse is an open-source discussion platform. Prior to version 3.2.3 on the `stable` branch and version 3.3.0.beta4 on the `beta` and `tests-passed` branches, moderators using the review queue to review users may see a users email address even when the Allow moderators to view email addresses setting is disabled. This issue is patched in version 3.2.3 on the `stable` branch and version 3.3.0.beta4 on the `beta` and `tests-passed` branches. As possible workarounds, either prevent moderators from accessing the review queue or disable the approve suspect users site setting and the must approve users site setting to prevent users from being added to the review queue.	2.4	More Details
CVE-2024-40594	The OpenAI ChatGPT app before 2024-07-05 for macOS opts out of the sandbox, and stores conversations in cleartext in a location accessible to other apps.	2.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38372	Undici is an HTTP/1.1 client, written from scratch for Node.js. Depending on network and process conditions of a `fetch()` request, `response.arrayBuffer()` might include portion of memory from the Node.js process. This has been patched in v6.19.2.	2.0	More Details
CVE-2024-22477	A cross-site scripting vulnerability exists in the admin console OIDC Policy Management Editor. The impact is contained to admin console users only.	1.8	More Details
CVE-2023-40702	PingOne MFA Integration Kit contains a vulnerability where the skipMFA action can be configured such that user authentication does not require the second factor authentication from the user's existing registered devices. A threat actor might be able to exploit this vulnerability to authenticate as a target user if they have existing knowledge of the target user's first-factor credentials.	N/A	More Details
CVE-2023-40356	PingOne MFA Integration Kit contains a vulnerability related to the Prompt Users to Set Up MFA configuration. Under certain conditions, this configuration could allow for a new MFA device to be paired with a target user account without requiring second-factor authentication from the target's existing registered devices. A threat actor might be able to exploit this vulnerability to register their own MFA device with a target user's account if they have existing knowledge of the target user's first factor credential.	N/A	More Details
CVE-2024-5821	The vulnerability allows an attacker to access sensitive files on the server by confusing the agent with incorrect file names. When a user requests the content of a file with a misspelled name, the agent attempts to correct the command and inadvertently reveals the content of the intended file, such as /etc/passwd. This can lead to unauthorized access to sensitive information and potential server compromise.	N/A	More Details
CVE-2024-5887	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-6488	Rejected reason: This is REJECTED.	N/A	More Details
CVE-2024-6461	Rejected reason: **REJECT** This is a duplicate CVE issued in error on a framework vulnerability. Please use CVE-2024-5324 instead.	N/A	More Details
CVE-2024-6463	Rejected reason: **REJECT** This is a duplicate CVE issued in error on a framework vulnerability. Please use CVE-2024-5324 instead.	N/A	More Details
CVE-2024-6464	Rejected reason: **REJECT** This is a duplicate CVE issued in error on a framework vulnerability. Please use CVE-2024-5324 instead.	N/A	More Details
CVE-2024-6284	In https://github.com/google/nftables IP addresses were encoded in the wrong byte order, resulting in an nftables configuration which does not work as intended (might block or not block the desired addresses). This issue affects: https://pkg.go.dev/github.com/google/nftables@v0.1.0 The bug was fixed in the next released version: https://pkg.go.dev/github.com/google/nftables@v0.2.0	N/A	More Details
CVE-2024-6513	Rejected reason: CVE assigned by mistake as a duplicate.	N/A	More Details
CVE-2024-5753	vanna-ai/vanna version v0.3.4 is vulnerable to SQL injection in some file-critical functions such as `pg_read_file()`. This vulnerability allows unauthenticated remote users to read arbitrary local files on the victim server, including sensitive files like `/etc/passwd`, by exploiting the exposed SQL queries via a Python Flask API.	N/A	More Details
CVE-2024-5616	A Cross-Site Request Forgery (CSRF) vulnerability exists in mudler/LocalAI versions up to and including 2.15.0, which allows attackers to trick victims into deleting installed models. By crafting a malicious HTML page, an attacker can cause the deletion of a model, such as 'gpt-4-vision-preview', without the victim's consent. The vulnerability is due to insufficient CSRF protection mechanisms on the model deletion functionality.	N/A	More Details
CVE-2024-4882	The user may be redirected to an arbitrary site in Sitefinity 15.1.8321.0 and previous versions.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6580	The /n software IPWorks SSH library SFTPServer component can be induced to make unintended filesystem or network path requests when loading a SSH public key or certificate. To be exploitable, an application calling the SFTPServer component must grant user access without verifying the SSH public key or certificate (which would most likely be a separate vulnerability in the calling application). IPWorks SSH versions 22.0.8945 and 24.0.8945 were released to address this condition by blocking all filesystem and network path requests for SSH public keys or certificates.	N/A	More Details
CVE-2024-5549	A CORS misconfiguration in the stitionai/devika repository allows attackers to steal sensitive information such as logs, browser sessions, and settings containing private API keys from other services. This vulnerability also enables attackers to perform actions on behalf of the user, such as deleting projects or sending messages. The issue arises from the lack of proper origin validation, allowing unauthorized cross-origin requests to be executed. The vulnerability is present in all versions of the repository, as no fixed version has been specified.	N/A	More Details
CVE-2024-5569	A Denial of Service (DoS) vulnerability exists in the jaraco/zipp library, affecting all versions prior to 3.19.1. The vulnerability is triggered when processing a specially crafted zip file that leads to an infinite loop. This issue also impacts the zipfile module of CPython, as features from the third-party zipp library are later merged into CPython, and the affected code is identical in both projects. The infinite loop can be initiated through the use of functions affecting the `Path` module in both zipp and zipfile, such as `joinpath`, the overloaded division operator, and `iterdir`. Although the infinite loop is not resource exhaustive, it prevents the application from responding. The vulnerability was addressed in version 3.19.1 of jaraco/zipp.	N/A	More Details
CVE-2024-22020	A security flaw in Node.js allows a bypass of network import restrictions. By embedding non-network imports in data URLs, an attacker can execute arbitrary code, compromising system security. Verified on various platforms, the vulnerability is mitigated by forbidding data URLs in network imports. Exploiting this flaw can violate network import security, posing a risk to developers and servers.	N/A	More Details
CVE-2024-34786	UniFi iOS app 10.15.0 introduces a misconfiguration on 2nd Generation UniFi Access Points configured as standalone (not using UniFi Network Application) that could cause the SSID name to change and/or the WiFi Password to be removed on the 5GHz Radio. This vulnerability is fixed in UniFi iOS app 10.15.2 and later.	N/A	More Details
CVE-2024-5631	Longse NVR (Network Video Recorder) model NVR3608PGE2W, as well as products based on this device, are transmitting user's login and password to a remote control service without using any encryption. This enables an on-path attacker to eavesdrop the credentials and subsequently obtain access to the video stream. The credentials are being sent when a user decides to change his password in router's portal.	N/A	More Details
CVE-2024-5632	Longse NVR (Network Video Recorder) model NVR3608PGE2W, as well as products based on this device, create a WiFi network with a default password. A user is neither advised to change it during the installation process, nor such a need is described in the manual. As the cameras from the same kit connect automatically, it is very probable for the default password to be left unchanged.	N/A	More Details
CVE-2024-5634	Longse model LBH30FE200W cameras, as well as products based on this device, make use of telnet passwords which follow a specific pattern. Once the pattern is known, brute-forcing the password becomes relatively easy. Additionally, every camera with the same firmware version shares the same password.	N/A	More Details
CVE-2024-6527	SQL Injection vulnerability in parameter "w" in file "druk.php" in MegaBIP software allows unauthorized attacker to disclose the contents of the database and obtain administrator's token to modify the content of pages. This issue affects MegaBIP software versions through 5.13.	N/A	More Details
CVE-2024-6598	A denial-of-service attack is possible through the execution functionality of KNIME Business Hub 1.10.0 and 1.10.1. It allows an authenticated attacker with job execution privileges to execute a job that causes internal messages to pile up until there are no more resources available for processing new messages. This leads to an outage of most functionality of KNIME Business Hub. Recovery from the situation is only possible by manual administrator interaction. Please contact our support for instructions in case you have run into this situation. Updating to KNIME Business Hub 1.10.2 or later solves the problem.	N/A	More Details
CVE-2024-5633	Longse model LBH30FE200W cameras, as well as products based on this device, provide an unrestricted access for an attacker located in the same local network to an undocumented binary service CoolView on one of the ports. An attacker with a knowledge of the available commands is able to perform read/write operations on the device's memory, which might result in e.g. bypassing telnet login and obtaining full access to the device.	N/A	More Details