SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 16 November 2022

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-2022-38650	A remote unauthenticated insecure deserialization vulnerability exists in VMware Hyperic Server 5.8.6. Exploitation of this vulnerability enables a malicious party to run arbitrary code or malware within Hyperic Server and the host operating system with the privileges of the Hyperic server process. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	10.0	More Details
CVE-2022-38652	A remote insecure deserialization vulnerability exixsts in VMWare Hyperic Agent 5.8.6. Exploitation of this vulnerability enables a malicious authenticated user to run arbitrary code or malware within a Hyperic Agent instance and its host operating system with the privileges of the Hyperic Agent process (often SYSTEM on Windows platforms). NOTE: prior exploitation of CVE-2022-38650 results in the disclosure of the authentication material required to exploit this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45182	Pi-Star_DV_Dash (for Pi-Star DV) before 5aa194d mishandles the module parameter.	9.8	More Details
CVE-2022-3362	Insufficient Session Expiration in GitHub repository ikus060/rdiffweb prior to 2.5.0.	9.8	More Details
CVE-2022-43671	Zoho ManageEngine Password Manager Pro before 12122, PAM360 before 5711, and Access Manager Plus before 4306 allow SQL Injection.	9.8	More Details
CVE-2022-43672	Zoho ManageEngine Password Manager Pro before 12122, PAM360 before 5711, and Access Manager Plus before 4306 allow SQL Injection (in a different software component relative to CVE-2022-43671.	9.8	More Details
CVE-2022-38651	A security filter misconfiguration exists in VMware Hyperic Server 5.8.6. Exploitation of this vulnerability enables a malicious party to bypass some authentication requirements when issuing requests to Hyperic Server. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2022-45378	In the default configuration of Apache SOAP, an RPCRouterServlet is available without authentication. This gives an attacker the possibility to invoke methods on the classpath that meet certain criteria. Depending on what classes are available on the classpath this might even lead to arbitrary remote code execution. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2022-3477	The tagDiv Composer WordPress plugin before 3.5, required by the Newspaper WordPress theme before 12.1 and Newsmag WordPress theme before 5.2.2, does not properly implement the Facebook login feature, allowing unauthenticated attackers to login as any user by just knowing their email address	9.8	More Details
CVE-2022-3574	The WPForms Pro WordPress plugin before 1.7.7 does not validate its form data when generating the exported CSV, which could lead to CSV injection.	9.8	More Details
CVE-2022-45136	Apache Jena SDB 3.17.0 and earlier is vulnerable to a JDBC Deserialisation attack if the attacker is able to control the JDBC URL used or cause the underlying database server to return malicious data. The mySQL JDBC driver in particular is known to be vulnerable to this class of attack. As a result an application using Apache Jena SDB can be subject to RCE when connected to a malicious database server. Apache Jena SDB has been EOL since December 2020 and users should migrate to alternative options e.g. Apache Jena TDB 2.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37109	patrickfuller camp up to and including commit bbd53a256ed70e79bd8758080936afbf6d738767 is vulnerable to Incorrect Access Control. Access to the password.txt file is not properly restricted as it is in the root directory served by StaticFileHandler and the Tornado rule to throw a 403 error when password.txt is accessed can be bypassed. Furthermore, it is not necessary to crack the password hash to authenticate with the application because the password hash is also used as the cookie secret, so an attacker can generate his own authentication cookie.	9.8	More Details
CVE-2022-43294	Tasmota before commit 066878da4d4762a9b6cb169fdf353e804d735cfd was discovered to contain a stack overflow via the ClientPortPtr parameter at lib/libesp32/rtsp/CRtspSession.cpp.	9.8	More Details
CVE-2022-36938	DexLoader function get_stringidx_fromdex() in Redex prior to commit 3b44c64 can load an out of bound address when loading the string index table, potentially allowing remote code execution during processing of a 3rd party Android APK file.	9.8	More Details
CVE-2022-42984	WoWonder Social Network Platform 4.1.4 was discovered to contain a SQL injection vulnerability via the offset parameter at requests.php?f=search&s=recipients.	9.8	More Details
CVE-2022-42120	A SQL injection vulnerability in the Fragment module in Liferay Portal 7.3.3 through 7.4.3.16, and Liferay DXP 7.3 before update 4, and 7.4 before update 17 allows attackers to execute arbitrary SQL commands via a PortletPreferences' `namespace` attribute.	9.8	More Details
CVE-2022-42122	A SQL injection vulnerability in the Friendly Url module in Liferay Portal 7.3.7, and Liferay DXP 7.3 fix pack 2 through update 4 allows attackers to execute arbitrary SQL commands via a crafted payload injected into the `title` field of a friendly URL.	9.8	More Details
CVE-2022-42058	Tenda AC1200 Router Model W15Ev2 V15.11.0.10(1576) was discovered to contain a stack overflow via the setRemoteWebManage function. This vulnerability allows attackers to cause a Denial of Service (DoS) via crafted overflow data.	9.8	More Details
CVE-2022-25727	Memory Corruption in modem due to improper length check while copying into memory in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music	9.8	More Details
CVE-2022-45395	Jenkins CCCC Plugin 0.6 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45396	Jenkins SourceMonitor Plugin 0.2 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	9.8	More Details
CVE-2022-45397	Jenkins OSF Builder Suite : : XML Linter Plugin 1.0.2 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	9.8	More Details
CVE-2022-45400	Jenkins JAPEX Plugin 1.7 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	9.8	More Details
CVE-2022-42785	Multiple W&T products of the ComServer Series are prone to an authentication bypass. An unathenticated remote attacker, can log in without knowledge of the password by crafting a modified HTTP GET Request.	9.8	More Details
CVE-2022-40797	Roxy Fileman 1.4.6 allows Remote Code Execution via a .phar upload, because the default FORBIDDEN_UPLOADS value in conf.json only blocks .php, .php4, and .php5 files. (Visiting any .phar file invokes the PHP interpreter in some realistic web-server configurations.)	9.8	More Details
CVE-2022-43265	An arbitrary file upload vulnerability in the component /pages/save_user.php of Canteen Management System v1.0 allows attackers to execute arbitrary code via a crafted PHP file.	9.8	More Details
CVE-2022-43074	AyaCMS v3.1.2 was discovered to contain an arbitrary file upload vulnerability via the component /admin/fst_upload.inc.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	9.8	More Details
CVE-2022-44559	The AMS module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation.	9.8	More Details
CVE-2022-45062	In Xfce xfce4-settings before 4.16.4 and 4.17.x before 4.17.1, there is an argument injection vulnerability in xfce4-mime-helper.	9.8	More Details
CVE-2021-34569	In WAGO I/O-Check Service in multiple products an attacker can send a specially crafted packet containing OS commands to crash the diagnostic tool and write memory.	9.8	More Details
CVE-2022-25932	The firmware of InHand Networks InRouter302 V3.5.45 introduces fixes for TALOS-2022-1472 and TALOS-2022-1474. The fixes are incomplete. An attacker can still perform, respectively, a privilege escalation and an information disclosure vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46851	The DRM module has a vulnerability in verifying the secure memory attributes. Successful exploitation of this vulnerability may cause abnormal video playback.	9.8	More Details
CVE-2022-31685	VMware Workspace ONE Assist prior to 22.10 contains an Authentication Bypass vulnerability. A malicious actor with network access to Workspace ONE Assist may be able to obtain administrative access without the need to authenticate to the application.	9.8	More Details
CVE-2022-31686	VMware Workspace ONE Assist prior to 22.10 contains a Broken Authentication Method vulnerability. A malicious actor with network access to Workspace ONE Assist may be able to obtain administrative access without the need to authenticate to the application.	9.8	More Details
CVE-2022-31687	VMware Workspace ONE Assist prior to 22.10 contains a Broken Access Control vulnerability. A malicious actor with network access to Workspace ONE Assist may be able to obtain administrative access without the need to authenticate to the application.	9.8	More Details
CVE-2022-31689	VMware Workspace ONE Assist prior to 22.10 contains a Session fixation vulnerability. A malicious actor who obtains a valid session token may be able to authenticate to the application using that token.	9.8	More Details
CVE-2022-43058	Online Diagnostic Lab Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /odlms//classes/Master.php?f=delete_activity.	9.8	More Details
CVE-2022-44558	The AMS module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation.	9.8	More Details
CVE-2022-44551	The iaware module has a vulnerability in thread security. Successful exploitation of this vulnerability will affect confidentiality, integrity, and availability.	9.8	More Details
CVE-2022-44562	The system framework layer has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation.	9.8	More Details
CVE-2022-39396	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Versions prior to 4.10.18, and prior to 5.3.1 on the 5.X branch, are vulnerable to Remote Code Execution via prototype pollution. An attacker can use this prototype pollution sink to trigger a remote code execution through the MongoDB BSON parser. This issue is patched in version 5.3.1 and in 4.10.18. There are no known workarounds.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38119	UPSMON Pro login function has insufficient authentication. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and get administrator privilege to access, control system or disrupt service.	9.8	More Details
CVE-2022-39036	The file upload function of Agentflow BPM has insufficient filtering for special characters in URLs. An unauthenticated remote attacker can exploit this vulnerability to upload arbitrary file and execute arbitrary code to manipulate system or disrupt service.	9.8	More Details
CVE-2022-44087	ESPCMS P8.21120101 was discovered to contain a remote code execution (RCE) vulnerability in the component UPFILE_PIC_ZOOM_HIGHT.	9.8	More Details
CVE-2022-44088	ESPCMS P8.21120101 was discovered to contain a remote code execution (RCE) vulnerability in the component INPUT_ISDESCRIPTION.	9.8	More Details
CVE-2022-44089	ESPCMS P8.21120101 was discovered to contain a remote code execution (RCE) vulnerability in the component IS_GETCACHE.	9.8	More Details
CVE-2022-45063	xterm before 375 allows code execution via font ops, e.g., because an OSC 50 response may have Ctrl-g and therefore lead to command execution within the vi line-editing mode of Zsh. NOTE: font ops are not allowed in the xterm default configurations of some Linux distributions.	9.8	More Details
CVE-2022-39395	Vela is a Pipeline Automation (CI/CD) framework built on Linux container technology written in Golang. In Vela Server and Vela Worker prior to version 0.16.0 and Vela UI prior to version 0.17.0, some default configurations for Vela allow exploitation and container breakouts. Users should upgrade to Server 0.16.0, Worker 0.16.0, and UI 0.17.0 to fix the issue. After upgrading, Vela administrators will need to explicitly change the default settings to configure Vela as desired. Some of the fixes will interrupt existing workflows and will require Vela administrators to modify default settings. However, not applying the patch (or workarounds) will continue existing risk exposure. Some workarounds are available. Vela administrators can adjust the worker's `VELA_RUNTIME_PRIVILEGED_IMAGES` setting to be explicitly empty, leverage the `VELA_REPO_ALLOWLIST` setting on the server component to restrict access to a list of repositories that are allowed to be enabled, and/or audit enabled repositories and disable pull_requests if they are not needed.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3890	Heap buffer overflow in Crashpad in Google Chrome on Android prior to 107.0.5304.106 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2022-3993	Improper Restriction of Excessive Authentication Attempts in GitHub repository kareadita/kavita prior to 0.6.0.3.	9.4	More Details
CVE-2021-34566	In WAGO I/O-Check Service in multiple products an unauthenticated remote attacker can send a specially crafted packet containing OS commands to crash the iocheck process and write memory resulting in loss of integrity and DoS.	9.1	More Details
CVE-2022-24942	Heap based buffer overflow in HTTP Server functionality in Micrium uC-HTTP 3.01.01 allows remote code execution via HTTP request.	9.1	More Details
CVE-2022-44727	The EU Cookie Law GDPR (Banner + Blocker) module before 2.1.3 for PrestaShop allows SQL Injection via a cookie (lgcookieslaw or __lglaw).	9.1	More Details
CVE-2022-41558	The Visualizations component of TIBCO Software Inc.'s TIBCO Spotfire Analyst, TIBCO Spotfire Analyst, TIBCO Spotfire Analyst, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Desktop, TIBCO Spotfire Desktop, TIBCO Spotfire Desktop, TIBCO Spotfire Server, TIBCO Spotfire Server, and TIBCO Spotfire Server contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute Stored Cross Site Scripting (XSS) on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analyst: versions 11.4.4 and below, TIBCO Spotfire Analyst: versions 11.5.0, 11.6.0, 11.7.0, 11.8.0, 12.0.0, and 12.0.1, TIBCO Spotfire Analyst: version 12.1.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 12.1.0 and below, TIBCO Spotfire Desktop: versions 11.4.4 and below, TIBCO Spotfire Desktop: versions 11.5.0, 11.6.0, 11.7.0, 11.8.0, 12.0.0, and 12.0.1, TIBCO Spotfire Desktop: version 12.1.0, TIBCO Spotfire Server: versions 11.4.8 and below, TIBCO Spotfire Server: versions 11.5.0, 11.6.0, 11.6.1, 11.6.2, 11.6.3, 11.7.0, 11.8.0, 11.8.1, 12.0.0, and 12.0.1, and TIBCO Spotfire Server: version 12.1.0.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2022-35613	Konker v2.3.9 was to discovered to contain a Cross-Site Request Forgery (CSRF).	8.8	More Details
CVE-2022-40127	A vulnerability in Example Dags of Apache Airflow allows an attacker with UI access who can trigger DAGs, to execute arbitrary commands via manually provided run_id parameter. This issue affects Apache Airflow Apache Airflow versions prior to 2.4.0.	8.8	More Details
CVE-2022-3240	The "Follow Me Plugin" plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.1.1. This is due to missing nonce validation on the FollowMeIgniteSocialMedia_options_page() function. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious JavaScript 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-2022-43288	Rukovoditel v3.2.1 was discovered to contain a SQL injection vulnerability via the order_by parameter at /rukovoditel/index.php?module=logs/view&type=php.	8.8	More Details
CVE-2022-42787	Multiple W&T products of the Comserver Series use a small number space for allocating sessions ids. After login of an user an unathenticated remote attacker can brute force the users session id and get access to his account on the the device. As the user needs to log in for the attack to be successful a user interaction is required.	8.8	More Details
CVE-2022-43693	Concrete CMS is vulnerable to CSRF due to the lack of "State" parameter for external Concrete authentication service for users of Concrete who use the "out of the box" core OAuth.	8.8	More Details
CVE-2022-28689	A leftover debug code vulnerability exists in the console support functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.	8.8	More Details
CVE-2022-43031	DedeCMS v6.1.9 was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to arbitrarily add Administrator accounts and modify Admin passwords.	8.8	More Details
CVE-2022-39038	Agentflow BPM enterprise management system has improper authentication. A remote attacker with general user privilege can change the name of the user account to acquire arbitrary account privilege, and access, manipulate system or disrupt service.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30543	A leftover debug code vulnerability exists in the console infct functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted series of network requests can lead to execution of privileged operations. An attacker can send a sequence of requests to trigger this vulnerability.	8.8	More Details
CVE-2022-3445	Use after free in Skia in Google Chrome prior to 106.0.5249.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-3446	Heap buffer overflow in WebSQL in Google Chrome prior to 106.0.5249.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-42121	A SQL injection vulnerability in the Layout module in Liferay Portal 7.1.3 through 7.4.3.4, and Liferay DXP 7.1 before fix pack 27, 7.2 before fix pack 17, 7.3 before service pack 3, and 7.4 GA allows remote authenticated attackers to execute arbitrary SQL commands via a crafted payload injected into a page template's 'Name' field.	8.8	More Details
CVE-2022-3448	Use after free in Permissions API in Google Chrome prior to 106.0.5249.119 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-3449	Use after free in Safe Browsing in Google Chrome prior to 106.0.5249.119 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High)	8.8	More Details
CVE-2022-3450	Use after free in Peer Connection in Google Chrome prior to 106.0.5249.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-43323	EyouCMS V1.5.9-UTF8-SP1 was discovered to contain a Cross-Site Request Forgery (CSRF) via the Top Up Balance component under the Edit Member module.	8.8	More Details
CVE-2022-41048	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-44387	EyouCMS V1.5.9-UTF8-SP1 was discovered to contain a Cross-Site Request Forgery (CSRF) via the Basic Information component under the Edit Member module.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39398	tasklists is a tasklists plugin for GLPI (Kanban). Versions prior to 2.0.3 are vulnerable to Cross-site Scripting. Cross-site Scripting (XSS) - Create XSS in task content (when add it). This issue is patched in version 2.0.3. There are no known workarounds.	8.8	More Details
CVE-2022-41047	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-3885	Use after free in V8 in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-3888	Use after free in WebCodecs in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-40773	Zoho ManageEngine ServiceDesk Plus MSP before 10609 and SupportCenter Plus before 11025 are vulnerable to privilege escalation. This allows users to obtain sensitive data during an exportMickeyList export of requests from the list view.	8.8	More Details
CVE-2020-12507	In s::can moni::tools before version 4.2 an authenticated attacker could get full access to the database through SQL injection. This may result in loss of confidentiality, loss of integrity and DoS.	8.8	More Details
CVE-2022-41062	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-41106	Microsoft Excel Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-3887	Use after free in Web Workers in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-3886	Use after free in Speech Recognition in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-41080	Microsoft Exchange Server Elevation of Privilege Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3889	Type confusion in V8 in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-45183	Escalation of privileges in the Web Server in Ironman Software PowerShell Universal 2.x and 3.x allows an attacker with a valid app token to retrieve other app tokens by ID via an HTTP web request. Patched Versions are 3.5.3, 3.4.7, and 2.12.6.	8.8	More Details
CVE-2022-41128	Windows Scripting Languages Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-33942	Protection mechanism failure in the Intel(R) DCM software before version 5.0 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2022-41978	Auth. (subscriber+) Arbitrary Options Update vulnerability in Zoho CRM Lead Magnet plugin <= 1.7.5.8 on WordPress.	8.8	More Details
CVE-2022-29277	Incorrect pointer checks within the the FwBlockServiceSmm driver can allow arbitrary RAM modifications During review of the FwBlockServiceSmm driver, certain instances of SpiAccessLib could be tricked into writing 0xff to arbitrary system and SMRAM addresses. Fixed in: INTEL Purley-R: 05.21.51.0048 Whitley: 05.42.23.0066 Cedar Island: 05.42.11.0021 Eagle Stream: 05.44.25.0052 Greenlow/Greenlow-R(skylake/kabylake): Trunk Mehlow/Mehlow-R (CoffeeLake-S): Trunk Tatlow (RKL-S): Trunk Denverton: 05.10.12.0042 Snow Ridge: Trunk Graneville DE: 05.05.15.0038 Grangeville DE NS: 05.27.26.0023 Bakerville: 05.21.51.0026 Idaville: 05.44.27.0030 Whiskey Lake: Trunk Comet Lake-S: Trunk Tiger Lake H/UP3: 05.43.12.0052 Alder Lake: 05.44.23.0047 Gemini Lake: Not Affected Apollo Lake: Not Affected Elkhart Lake: 05.44.30.0018 AMD ROME: trunk MILAN: 05.36.10.0017 GENOA: 05.52.25.0006 Snowy Owl: Trunk R1000: 05.32.50.0018 R2000: 05.44.30.0005 V2000: Trunk V3000: 05.44.30.0007 Ryzen 5000: 05.44.30.0004 Embedded ROME: Trunk Embedded MILAN: Trunk Hygon Hygon #1/#2: 05.36.26.0016 Hygon #3: 05.44.26.0007 https://www.insyde.com/security-pledge/SA-2022060	8.8	More Details
CVE-2022-26845	Improper authentication in firmware for Intel(R) AMT before versions 11.8.93, 11.22.93, 11.12.93, 12.0.92, 14.1.67, 15.0.42, 16.1.25 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41906	OpenSearch Notifications is a notifications plugin for OpenSearch that enables other plugins to send notifications via Email, Slack, Amazon Chime, Custom web-hook etc channels. A potential SSRF issue in OpenSearch Notifications Plugin starting in 2.0.0 and prior to 2.2.1 could allow an existing privileged user to enumerate listening services or interact with configured resources via HTTP requests exceeding the Notification plugin's intended scope. OpenSearch 2.2.1+ contains the fix for this issue. There are currently no recommended workarounds.	8.7	More Details
CVE-2022-20947	A vulnerability in dynamic access policies (DAP) functionality of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to improper processing of HostScan data received from the Posture (HostScan) module. An attacker could exploit this vulnerability by sending crafted HostScan data to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dap-dos-GhYZBxDU ["https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dap-dos-GhYZBxDU"] This advisory is part of the November 2022 release of the Cisco ASA, FTD, and FMC Security Advisory Bundled publication.	8.6	More Details
CVE-2022-20946	A vulnerability in the generic routing encapsulation (GRE) tunnel decapsulation feature of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to a memory handling error that occurs when GRE traffic is processed. An attacker could exploit this vulnerability by sending a crafted GRE payload through an affected device. A successful exploit could allow the attacker to cause the device to restart, resulting in a DoS condition. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-gre-dos-hmedHQPM ["https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-gre-dos-hmedHQPM"] This advisory is part of the November 2022 release of the Cisco ASA, FTD, and FMC Security Advisory Bundled publication.	8.6	More Details
CVE-2022-41892	Arches is a web platform for creating, managing, & visualizing geospatial data. Versions prior to 6.1.2, 6.2.1, and 7.1.2 are vulnerable to SQL Injection. With a carefully crafted web request, it's possible to execute certain unwanted sql statements against the database. This issue is fixed in version 7.12, 6.2.1, and 6.1.2. Users are recommended to upgrade as soon as possible. There are no workarounds.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39393	Wasmtime is a standalone runtime for WebAssembly. Prior to version 2.0.2, there is a bug in Wasmtime's implementation of its pooling instance allocator where when a linear memory is reused for another instance the initial heap snapshot of the prior instance can be visible, erroneously to the next instance. This bug has been patched and users should upgrade to Wasmtime 2.0.2. Other mitigations include disabling the pooling allocator and disabling the `memory-init-cow`.	8.6	More Details
CVE-2022-27497	Null pointer dereference in firmware for Intel(R) AMT before version 11.8.93, 11.22.93, 11.12.93, 12.0.92, 14.1.67, 15.0.42, 16.1.25 may allow an unauthenticated user to potentially enable denial of service via network access.	8.6	More Details
CVE-2022-25724	Memory corruption in graphics due to buffer overflow while validating the user address in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2022-25743	Memory corruption in graphics due to use-after-free while importing graphics buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2022-39368	Eclipse Californium is a Java implementation of RFC7252 - Constrained Application Protocol for IoT Cloud services. In versions prior to 3.7.0, and 2.7.4, Californium is vulnerable to a Denial of Service. Failing handshakes don't cleanup counters for throttling, causing the threshold to be reached without being released again. This results in permanently dropping records. The issue was reported for certificate based handshakes, but may also affect PSK based handshakes. It generally affects client and server as well. This issue is patched in version 3.7.0 and 2.7.4. There are no known workarounds. main: commit 726bac57659410da463dcf404b3e79a7312ac0b9 2.7.x: commit 5648a0c27c2c2667c98419254557a14bac2b1f3f	8.2	More Details
CVE-2022-30771	Initialization function in PnpSmm could lead to SMRAM corruption when using subsequent PNP SMI functions Initialization function in PnpSmm could lead to SMRAM corruption when using subsequent PNP SMI functions. This issue was discovered by Insyde engineering during a security review. Fixed in: Kernel 5.1: Version 05.17.25 Kernel 5.2: Version 05.27.25 Kernel 5.3: Version 05.36.25 Kernel 5.4: Version 05.44.25 Kernel 5.5: Version 05.52.25 https://www.insyde.com/security-pledge/SA-2022064	8.2	More Details
CVE-2021-33164	Improper access control in BIOS firmware for some Intel(R) NUCs before version INWHL357.0046 may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30542	Improper input validation in the firmware for some Intel(R) Server Board S2600WF, Intel(R) Server System R1000WF and Intel(R) Server System R2000WF families before version R02.01.0014 may allow a privileged user to potentially enable an escalation of privilege via local access.	8.2	More Details
CVE-2022-41905	WsgiDAV is a generic and extendable WebDAV server based on WSGI. Implementations using this library with directory browsing enabled may be susceptible to Cross Site Scripting (XSS) attacks. This issue has been patched, users can upgrade to version 4.1.0. As a workaround, set `dir_browser.enable = False` in the configuration.	8.2	More Details
CVE-2022-29279	Use of a untrusted pointer allows tampering with SMRAM and OS memory in SdHostDriver and SdMmcDevice Use of a untrusted pointer allows tampering with SMRAM and OS memory in SdHostDriver and SdMmcDevice. This issue was discovered by Insyde during security review. It was fixed in: Kernel 5.0: version 05.09.17 Kernel 5.1: version 05.17.17 Kernel 5.2: version 05.27.17 Kernel 5.3: version 05.36.17 Kernel 5.4: version 05.44.17 Kernel 5.5: version 05.52.17 https://www.insyde.com/security-pledge/SA-2022062	8.2	More Details
CVE-2022-29278	Incorrect pointer checks within the NvmExpressDxe driver can allow tampering with SMRAM and OS memory Incorrect pointer checks within the NvmExpressDxe driver can allow tampering with SMRAM and OS memory. This issue was discovered by Insyde during security review. Fixed in: Kernel 5.1: Version 05.17.23 Kernel 5.2: Version 05.27.23 Kernel 5.3: Version 05.36.23 Kernel 5.4: Version 05.44.23 Kernel 5.5: Version 05.52.23 https://www.insyde.com/security-pledge/SA-2022061	8.2	More Details
CVE-2021-34567	In WAGO I/O-Check Service in multiple products an unauthenticated remote attacker can send a specially crafted packet containing OS commands to provoke a denial of service and an limited out-of-bounds read.	8.2	More Details
CVE-2022-29276	SMI functions in AhciBusDxe use untrusted inputs leading to corruption of SMRAM. SMI functions in AhciBusDxe use untrusted inputs leading to corruption of SMRAM. This issue was discovered by Insyde during security review. It was fixed in: Kernel 5.0: version 05.09.18 Kernel 5.1: version 05.17.18 Kernel 5.2: version 05.27.18 Kernel 5.3: version 05.36.18 Kernel 5.4: version 05.44.18 Kernel 5.5: version 05.52.18 https://www.insyde.com/security-pledge/SA-2022059	8.2	More Details
CVE-2022-33176	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Performance kits and Intel(R) NUC 11 Performance Mini PCs before version PATGL357.0042 may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30772	Manipulation of the input address in PnpSmm function 0x52 could be used by malware to overwrite SMRAM or OS kernel memory. Function 0x52 of the PnpSmm driver is passed the address and size of data to write into the SMBIOS table, but manipulation of the address could be used by malware to overwrite SMRAM or OS kernel memory. This issue was discovered by Insyde engineering during a security review. This issue is fixed in: Kernel 5.0: 05.09.41 Kernel 5.1: 05.17.43 Kernel 5.2: 05.27.30 Kernel 5.3: 05.36.30 Kernel 5.4: 05.44.30 Kernel 5.5: 05.52.30 https://www.insyde.com/security-pledge/SA-2022065	8.2	More Details
CVE-2022-26006	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2022-26341	Insufficiently protected credentials in software in Intel(R) AMT SDK before version 16.0.4.1, Intel(R) EMA before version 1.7.1 and Intel(R) MC before version 2.3.2 may allow an authenticated user to potentially enable escalation of privilege via network access.	8.2	More Details
CVE-2022-29275	In UsbCoreDxe, untrusted input may allow SMRAM or OS memory tampering Use of untrusted pointers could allow OS or SMRAM memory tampering leading to escalation of privileges. This issue was discovered by Insyde during security review. It was fixed in: Kernel 5.0: version 05.09.21 Kernel 5.1: version 05.17.21 Kernel 5.2: version 05.27.21 Kernel 5.3: version 05.36.21 Kernel 5.4: version 05.44.21 Kernel 5.5: version 05.52.21 https://www.insyde.com/security-pledge/SA-2022058	8.2	More Details
CVE-2022-29888	A leftover debug code vulnerability exists in the httpd port 4444 upload.cgi functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted HTTP request can lead to arbitrary file deletion. An attacker can send an HTTP request to trigger this vulnerability.	8.1	More Details
CVE-2022-38023	Netlogon RPC Elevation of Privilege Vulnerability	8.1	More Details
CVE-2022-37966	Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability	8.1	More Details
CVE-2022-41088	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45381	Jenkins Pipeline Utility Steps Plugin 2.13.1 and earlier does not restrict the set of enabled prefix interpolators and bundles versions of Apache Commons Configuration library that enable the 'file:' prefix interpolator by default, allowing attackers able to configure Pipelines to read arbitrary files from the Jenkins controller file system.	8.1	More Details
CVE-2022-41039	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-41044	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-29893	Improper authentication in firmware for Intel(R) AMT before versions 11.8.93, 11.22.93, 11.12.93, 12.0.92, 14.1.67, 15.0.42, 16.1.25 may allow an authenticated user to potentially enable escalation of privilege via network access.	8.1	More Details
CVE-2022-0324	There is a vulnerability in DHCPv6 packet parsing code that could be explored by remote attacker to craft a packet that could cause buffer overflow in a memcpy call, leading to out-of-bounds memory write that would cause dhcp6relay to crash. Dhcp6relay is a critical process and could cause dhcp relay docker to shutdown. Discovered by Eugene Lim of GovTech Singapore.	8.1	More Details
CVE-2022-39882	Heap overflow vulnerability in sflacf_fal_bytes_peek function in libsmat.so library prior to SMR Nov-2022 Release 1 allows local attacker to execute arbitrary code.	8.0	More Details
CVE-2022-41079	Microsoft Exchange Server Spoofing Vulnerability	8.0	More Details
CVE-2022-26513	Out-of-bounds write in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.0	More Details
CVE-2022-41078	Microsoft Exchange Server Spoofing Vulnerability	8.0	More Details
CVE-2022-21198	Time-of-check time-of-use race condition in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	7.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41073	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-41063	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-3737	In PHOENIX CONTACT Automationworx Software Suite up to version 1.89 memory can be read beyond the intended scope due to insufficient validation of input data. Availability, integrity, or confidentiality of an application programming workstation might be compromised by attacks using these vulnerabilities.	7.8	More Details
CVE-2022-41092	Windows Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-41093	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-41095	Windows Digital Media Receiver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-41096	Microsoft DWM Core Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-41123	Microsoft Exchange Server Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-3461	In PHOENIX CONTACT Automationworx Software Suite up to version 1.89 manipulated PC Worx or Config+ files could lead to a heap buffer overflow and a read access violation. Availability, integrity, or confidentiality of an application programming workstation might be compromised by attacks using these vulnerabilities.	7.8	More Details
CVE-2022-42053	Tenda AC1200 Router Model W15Ev2 V15.11.0.10(1576) was discovered to contain a command injection vulnerability via the PortMappingServer parameter in the setPortMapping function.	7.8	More Details
CVE-2022-37345	Improper authentication in BIOS firmware[A1] for some Intel(R) NUC Kits before version RY0386 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37334	Improper initialization in BIOS firmware for some Intel(R) NUC 11 Pro Kits and Intel(R) NUC 11 Pro Boards before version TNTGL357.0064 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-3238	A double-free flaw was found in the Linux kernel's NTFS3 subsystem in how a user triggers remount and umount simultaneously. This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.8	More Details
CVE-2022-34325	DMA transactions which are targeted at input buffers used for the StorageSecurityCommandDxe software SMI handler could cause SMRAM corruption through a TOCTOU attack. DMA transactions which are targeted at input buffers used for the software SMI handler used by the StorageSecurityCommandDxe driver could cause SMRAM corruption. This issue was discovered by Insyde engineering based on the general description provided by	7.8	More Details
CVE-2022-41057	Windows HTTP.sys Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-40847	In Tenda AC1200 Router model W15Ev2 V15.11.0.10(1576), there exists a command injection vulnerability in the function formSetFixTools. This vulnerability allows attackers to run arbitrary commands on the server via the hostname parameter.	7.8	More Details
CVE-2022-41395	Tenda AC1200 Router Model W15Ev2 V15.11.0.10(1576) was discovered to contain a command injection vulnerability via the dmzHost parameter in the setDMZ function.	7.8	More Details
CVE-2022-41396	Tenda AC1200 Router Model W15Ev2 V15.11.0.10(1576) was discovered to contain multiple command injection vulnerabilities in the function setIPsecTunnelList via the IPsecLocalNet and IPsecRemoteNet parameters.	7.8	More Details
CVE-2022-41125	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-41100	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-45188	Netatalk through 3.1.13 has an afp_getappl heap-based buffer overflow resulting in code execution via a crafted .appl file. This provides remote root access on some platforms such as FreeBSD (used for TrueNAS).	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41120	Microsoft Windows System Monitor (Sysmon) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-41119	Visual Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-41113	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-41109	Windows Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-41107	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-41102	Windows Overlay Filter Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-41101	Windows Overlay Filter Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-41061	Microsoft Word Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-41339	In Zoho ManageEngine Mobile Device Manager Plus before 10.1.2207.5, the User Administration module allows privilege escalation.	7.8	More Details
CVE-2021-26392	Insufficient verification of missing size check in 'LoadModule' may lead to an out-of-bounds write potentially allowing an attacker with privileges to gain code execution of the OS/kernel by loading a malicious TA.	7.8	More Details
CVE-2022-41050	Windows Extensible File Allocation Table Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3377	Horner Automation's Cscape version 9.90 SP 6 and prior does not properly validate user-supplied data. If a user opens a maliciously formed FNT file, then an attacker could execute arbitrary code within the current process by accessing an uninitialized pointer, leading to an out-of-bounds memory read.	7.8	More Details
CVE-2022-37992	Windows Group Policy Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-32588	An out-of-bounds write vulnerability exists in the PICT parsing pctwread_14841 functionality of Accusoft ImageGear 20.0. A specially-crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2022-41045	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-12931	Improper parameters handling in the AMD Secure Processor (ASP) kernel may allow a privileged attacker to elevate their privileges potentially leading to loss of integrity.	7.8	More Details
CVE-2020-12930	Improper parameters handling in AMD Secure Processor (ASP) drivers may allow a privileged attacker to elevate their privileges potentially leading to loss of integrity.	7.8	More Details
CVE-2022-41051	Azure RTOS GUIX Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-26391	Insufficient verification of multiple header signatures while loading a Trusted Application (TA) may allow an attacker with privileges to gain code execution in that TA or the OS/kernel.	7.8	More Details
CVE-2022-41054	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-26360	An attacker with local access to the system can make unauthorized modifications of the security configuration of the SOC registers. This could allow potential corruption of AMD secure processor’s encrypted memory contents which may lead to arbitrary code execution in ASP.	7.8	More Details
CVE-2022-41052	Windows Graphics Component Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43310	An Uncontrolled Search Path Element in Foxit Software released Foxit Reader v11.2.118.51569 allows attackers to escalate privileges when searching for DLL libraries without specifying an absolute path.	7.8	More Details
CVE-2022-21794	Improper authentication in BIOS firmware for some Intel(R) NUC Boards, Intel(R) NUC Business, Intel(R) NUC Enthusiast, Intel(R) NUC Kits before version HN0067 may allow a privileged user to potentially enable escalation of privilege via local access.	7.7	More Details
CVE-2022-20927	A vulnerability in the SSL/TLS client of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper memory management when a device initiates SSL/TLS connections. An attacker could exploit this vulnerability by ensuring that the device will connect to an SSL/TLS server that is using specific encryption parameters. A successful exploit could allow the attacker to cause the affected device to unexpectedly reload, resulting in a DoS condition.	7.7	More Details
CVE-2022-20924	A vulnerability in the Simple Network Management Protocol (SNMP) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	7.7	More Details
CVE-2022-34152	Improper input validation in BIOS firmware for some Intel(R) NUC Boards, Intel(R) NUC Kits before version TY0070 may allow a privileged user to potentially enable escalation of privilege via local access.	7.7	More Details
CVE-2022-39388	Istio is an open platform to connect, manage, and secure microservices. In versions on the 1.15.x branch prior to 1.15.3, a user can impersonate any workload identity within the service mesh if they have localhost access to the Istiod control plane. Version 1.15.3 contains a patch for this issue. There are no known workarounds.	7.6	More Details
CVE-2022-3703	All versions of ETIC Telecom Remote Access Server (RAS) 4.5.0 and prior's web portal is vulnerable to accepting malicious firmware packages that could provide a backdoor to an attacker and provide privilege escalation to the device.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42977	The Netic User Export add-on before 1.3.5 for Atlassian Confluence has the functionality to generate a list of users in the application, and export it. During export, the HTTP request has a fileName parameter that accepts any file on the system (e.g., an SSH private key) to be downloaded.	7.5	More Details
CVE-2022-39037	Agentflow BPM file download function has a path traversal vulnerability. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and download arbitrary system files.	7.5	More Details
CVE-2022-38122	UPSMON PRO transmits sensitive data in cleartext over HTTP protocol. An unauthenticated remote attacker can exploit this vulnerability to access sensitive data.	7.5	More Details
CVE-2021-34568	In WAGO I/O-Check Service in multiple products an unauthenticated remote attacker can send a specially crafted packet containing OS commands to provoke a denial of service.	7.5	More Details
CVE-2022-27949	A vulnerability in UI of Apache Airflow allows an attacker to view unmasked secrets in rendered template values for tasks which were not executed (for example when they were depending on past and previous instances of the task failed). This issue affects Apache Airflow prior to 2.3.1.	7.5	More Details
CVE-2022-44546	The kernel module has the vulnerability that the mapping is not cleared after the memory is automatically released. Successful exploitation of this vulnerability may cause a system restart.	7.5	More Details
CVE-2022-42978	In the Netic User Export add-on before 1.3.5 for Atlassian Confluence, authorization is mishandled. An unauthenticated attacker could access files on the remote system.	7.5	More Details
CVE-2022-45129	Payara before 2022-11-04, when deployed to the root context, allows attackers to visit META-INF and WEB-INF, a different vulnerability than CVE-2022-37422. This affects Payara Platform Community before 4.1.2.191.38, 5.x before 5.2022.4, and 6.x before 6.2022.1, and Payara Platform Enterprise before 5.45.0.	7.5	More Details
CVE-2022-35276	Improper access control in BIOS firmware for some Intel(R) NUC 8 Compute Elements before version CBWHL357.0096 may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2022-44547	The Display Service module has a UAF vulnerability. Successful exploitation of this vulnerability may affect the display service availability.	7.5	More Details
CVE-2022-44549	The LBS module has a vulnerability in geofencing API access. Successful exploitation of this vulnerability may cause third-party apps to access the geofencing APIs without authorization, affecting user confidentiality.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44550	The graphics display module has a UAF vulnerability when traversing graphic layers. Successful exploitation of this vulnerability may affect system availability.	7.5	More Details
CVE-2022-42060	Tenda AC1200 Router Model W15Ev2 V15.11.0.10(1576) was discovered to contain a stack overflow via the setWanPpoe function. This vulnerability allows attackers to cause a Denial of Service (DoS) via crafted overflow data.	7.5	More Details
CVE-2022-42125	Zip slip vulnerability in FileUtil.unzip in Liferay Portal 7.4.3.5 through 7.4.3.35 and Liferay DXP 7.4 update 1 through update 34 allows attackers to create or overwrite existing files on the filesystem via the deployment of a malicious plugin/module.	7.5	More Details
CVE-2022-27673	Insufficient access controls in the AMD Link Android app may potentially result in information disclosure.	7.5	More Details
CVE-2022-42124	ReDoS vulnerability in LayoutPageTemplateEntryUpgradeProcess in Liferay Portal 7.3.2 through 7.4.3.4 and Liferay DXP 7.2 fix pack 9 through fix pack 18, 7.3 before update 4, and DXP 7.4 GA allows remote attackers to consume an excessive amount of server resources via a crafted payload injected into the 'name' field of a layout prototype.	7.5	More Details
CVE-2022-41056	Network Policy Server (NPS) RADIUS Protocol Denial of Service Vulnerability	7.5	More Details
CVE-2022-40735	The Diffie-Hellman Key Agreement Protocol allows use of long exponents that arguably make certain calculations unnecessarily expensive, because the 1996 van Oorschot and Wiener paper found that "(appropriately) short exponents" can be used when there are adequate subgroup constraints, and these short exponents can lead to less expensive calculations than for long exponents. This issue is different from CVE-2002-20001 because it is based on an observation about exponent size, rather than an observation about numbers that are not public keys. The specific situations in which calculation expense would constitute a server-side vulnerability depend on the protocol (e.g., TLS, SSH, or IKE) and the DHE implementation details. In general, there might be an availability concern because of server-side resource consumption from DHE modular-exponentiation calculations. Finally, it is possible for an attacker to exploit this vulnerability and CVE-2002-20001 together.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30283	In UsbCoreDxe, tampering with the contents of the USB working buffer using DMA while certain USB transactions are in process leads to a TOCTOU problem that could be used by an attacker to cause SMRAM corruption and escalation of privileges The UsbCoreDxe module creates a working buffer for USB transactions outside of SMRAM. The code which uses can be inside of SMM, making the working buffer untrusted input. The buffer can be corrupted by DMA transfers. The SMM code code attempts to sanitize pointers to ensure all pointers refer to the working buffer, but when a pointer is not found in the list of pointers to sanitize, the current action is not aborted, leading to undefined behavior. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. Fixed in: Kernel 5.0: Version 05.09. 21 Kernel 5.1: Version 05.17.21 Kernel 5.2: Version 05.27.21 Kernel 5.3: Version 05.36.21 Kernel 5.4: Version 05.44.21 Kernel 5.5: Version 05.52.21 https://www.insyde.com/security-pledge/SA-2022063	7.5	More Details
CVE-2022-26124	Improper buffer restrictions in BIOS firmware for some Intel(R) NUC Boards, Intel(R) NUC 8 Boards, Intel(R) NUC 8 Rugged Boards and Intel(R) NUC 8 Rugged Kits before version CHAPLCEL.0059 may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2021-46852	The memory management module has the logic bypass vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2021-0185	Improper input validation in the firmware for some Intel(R) Server Board M10JNP Family before version 7.216 may allow a privileged user to potentially enable an escalation of privilege via local access.	7.5	More Details
CVE-2022-0137	A heap buffer overflow in image_set_mask function of HTMLDOC before 1.9.15 allows an attacker to write outside the buffer boundaries.	7.5	More Details
CVE-2021-34579	In Phoenix Contact: FL MGUARD DM version 1.12.0 and 1.13.0 access to the Apache web server being installed as part of the FL MGUARD DM on Microsoft Windows does not require login credentials even if configured during installation.Attackers with network access to the Apache web server can download and therefore read mGuard configuration profiles (“ATV profiles”). Such configuration profiles may contain sensitive information, e.g. private keys associated with IPsec VPN connections.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41876	ezplatform-graphql is a GraphQL server implementation for Ibexa DXP and Ibexa Open Source. Versions prior to 2.3.12 and 1.0.13 are subject to Insecure Storage of Sensitive Information. Unauthenticated GraphQL queries for user accounts can expose password hashes of users that have created or modified content, typically administrators and editors. This issue has been patched in versions 2.3.12, and 1.0.13 on the 1.X branch. Users unable to upgrade can remove the "passwordHash" entry from "src/bundle/Resources/config/graphql/User.types.yaml" in the GraphQL package, and other properties like hash type, email, login if you prefer.	7.5	More Details
CVE-2021-40226	xpdfreader 4.03 is vulnerable to Buffer Overflow.	7.5	More Details
CVE-2022-32569	Improper buffer restrictions in BIOS firmware for some Intel(R) NUC M15 Laptop Kits before version BCTGL357.0074 may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2022-41719	Unmarshal can panic on some inputs, possibly allowing for denial of service attacks.	7.5	More Details
CVE-2022-23831	Insufficient validation of the IOCTL input buffer in AMD µProf may allow an attacker to send an arbitrary buffer leading to a potential Windows kernel crash resulting in denial of service.	7.5	More Details
CVE-2022-44552	The lock screen module has defects introduced in the design process. Successful exploitation of this vulnerability may affect system availability.	7.5	More Details
CVE-2022-40405	WoWonder Social Network Platform v4.1.2 was discovered to contain a SQL injection vulnerability via the offset parameter at requests.php?f=load-my-blogs.	7.5	More Details
CVE-2022-27674	Insufficient validation in the IOCTL input/output buffer in AMD µProf may allow an attacker to bypass bounds checks potentially leading to a Windows kernel crash resulting in denial of service.	7.5	More Details
CVE-2022-42123	A Zip slip vulnerability in the Elasticsearch Connector in Liferay Portal 7.3.3 through 7.4.3.18, and Liferay DXP 7.3 before update 6, and 7.4 before update 19 allows attackers to create or overwrite existing files on the filesystem via the installation of a malicious Elasticsearch Sidecar plugin.	7.5	More Details
CVE-2022-25671	Denial of service in MODEM due to reachable assertion in Snapdragon Mobile	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36370	Improper authentication in BIOS firmware for some Intel(R) NUC Boards and Intel(R) NUC Kits before version MYi30060 may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2022-25667	Information disclosure in kernel due to improper handling of ICMP requests in Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2022-45379	Jenkins Script Security Plugin 1189.vb_a_b_7c8fd5fde and earlier stores whole-script approvals as the SHA-1 hash of the script, making it vulnerable to collision attacks.	7.5	More Details
CVE-2022-45198	Pillow before 9.2.0 performs Improper Handling of Highly Compressed GIF Data (Data Amplification).	7.5	More Details
CVE-2022-33236	Transient DOS due to buffer over-read in WLAN firmware while parsing cipher suite info attributes. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2022-33237	Transient DOS due to buffer over-read in WLAN firmware while processing PPE threshold. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2021-38827	Xiongmai Camera XM-JPR2-LX V4.02.R12.A6420987.10002.147502.00000 is vulnerable to account takeover.	7.5	More Details
CVE-2022-20854	A vulnerability in the processing of SSH connections of Cisco Firepower Management Center (FMC) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper error handling when an SSH session fails to be established. An attacker could exploit this vulnerability by sending a high rate of crafted SSH connections to the instance. A successful exploit could allow the attacker to cause resource exhaustion, resulting in a reboot on the affected device.	7.5	More Details
CVE-2022-38666	Jenkins NS-ND Integration Performance Publisher Plugin 4.8.0.146 and earlier unconditionally disables SSL/TLS certificate and hostname validation for several features.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33239	Transient DOS due to loop with unreachable exit condition in WLAN firmware while parsing IPV6 extension header. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2022-45196	Hyperledger Fabric 2.3 allows attackers to cause a denial of service (orderer crash) by repeatedly sending a crafted channel tx with the same Channel name. NOTE: the official Fabric with Raft prevents exploitation via a locking mechanism and a check for names that already exist.	7.5	More Details
CVE-2022-40308	If anonymous read enabled, it's possible to read the database file directly without logging in.	7.5	More Details
CVE-2020-12508	In s::can moni::tools in versions below 4.2 an unauthenticated attacker could get any file from the device by path traversal in the image-relocator module.	7.5	More Details
CVE-2022-41085	Azure CycleCloud Elevation of Privilege Vulnerability	7.5	More Details
CVE-2022-45060	An HTTP Request Forgery issue was discovered in Varnish Cache 5.x and 6.x before 6.0.11, 7.x before 7.1.2, and 7.2.x before 7.2.1. An attacker may introduce characters through HTTP/2 pseudo-headers that are invalid in the context of an HTTP/1 request line, causing the Varnish server to produce invalid HTTP/1 requests to the backend. This could, in turn, be used to exploit vulnerabilities in a server behind the Varnish server. Note: the 6.0.x LTS series (before 6.0.11) is affected.	7.5	More Details
CVE-2022-45061	An issue was discovered in Python before 3.11.1. An unnecessary quadratic algorithm exists in one path when processing some inputs to the IDNA (RFC 3490) decoder, such that a crafted, unreasonably long name being presented to the decoder could lead to a CPU denial of service. Hostnames are often supplied by remote servers that could be controlled by a malicious actor; in such a scenario, they could trigger excessive CPU consumption on the client attempting to make use of an attacker-supplied supposed hostname. For example, the attack payload could be placed in the Location header of an HTTP response with status code 302. A fix is planned in 3.11.1, 3.10.9, 3.9.16, 3.8.16, and 3.7.16.	7.5	More Details
CVE-2022-45391	Jenkins NS-ND Integration Performance Publisher Plugin 4.8.0.143 and earlier globally and unconditionally disables SSL/TLS certificate and hostname validation for the entire Jenkins controller JVM.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45388	Jenkins Config Rotator Plugin 2.0.1 and earlier does not restrict a file name query parameter in an HTTP endpoint, allowing unauthenticated attackers to read arbitrary files with '.xml' extension on the Jenkins controller file system.	7.5	More Details
CVE-2022-3480	A remote, unauthenticated attacker could cause a denial-of-service of PHOENIX CONTACT FL MGUARD and TC MGUARD devices below version 8.9.0 by sending a larger number of unauthenticated HTTPS connections originating from different source IP's. Configuring firewall limits for incoming connections cannot prevent the issue.	7.5	More Details
CVE-2022-45199	Pillow before 9.3.0 allows denial of service via SAMPLESPERPIXEL.	7.5	More Details
CVE-2022-45385	A missing permission check in Jenkins CloudBees Docker Hub/Registry Notification Plugin 2.6.2 and earlier allows unauthenticated attackers to trigger builds of jobs corresponding to the attacker-specified repository.	7.5	More Details
CVE-2022-41053	Windows Kerberos Denial of Service Vulnerability	7.5	More Details
CVE-2022-20918	A vulnerability in the Simple Network Management Protocol (SNMP) access controls for Cisco FirePOWER Software for Adaptive Security Appliance (ASA) FirePOWER module, Cisco Firepower Management Center (FMC) Software, and Cisco Next-Generation Intrusion Prevention System (NGIPS) Software could allow an unauthenticated, remote attacker to perform an SNMP GET request using a default credential. This vulnerability is due to the presence of a default credential for SNMP version 1 (SNMPv1) and SNMP version 2 (SNMPv2). An attacker could exploit this vulnerability by sending an SNMPv1 or SNMPv2 GET request to an affected device. A successful exploit could allow the attacker to retrieve sensitive information from the device using the default credential. This attack will only be successful if SNMP is configured, and the attacker can only perform SNMP GET requests; write access using SNMP is not allowed.	7.5	More Details
CVE-2022-41118	Windows Scripting Languages Remote Code Execution Vulnerability	7.5	More Details
CVE-2022-44561	The preset launcher module has a permission verification vulnerability. Successful exploitation of this vulnerability makes unauthorized apps add arbitrary widgets and shortcuts without interaction.	7.5	More Details
CVE-2022-38099	Improper input validation in BIOS firmware for some Intel(R) NUC 11 Compute Elements before version EBTGL357.0065 may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44557	The SmartTrimProcessEvent module has a vulnerability of obtaining the read and write permissions on arbitrary system files. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-44555	The DDMP/ODMF module has a service hijacking vulnerability. Successful exploit of this vulnerability may cause services to be unavailable.	7.5	More Details
CVE-2022-44554	The power module has a vulnerability in permission verification. Successful exploitation of this vulnerability may cause abnormal status of a module on the device.	7.5	More Details
CVE-2022-25710	Denial of service due to null pointer dereference when GATT is disconnected in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	7.5	More Details
CVE-2022-36789	Improper access control in BIOS firmware for some Intel(R) NUC 10 Performance Kits and Intel(R) NUC 10 Performance Mini PCs before version FNCML357.0053 may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2022-25742	Denial of service in modem due to infinite loop while parsing IGMPv2 packet from server in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music	7.5	More Details
CVE-2022-25741	Denial of service in WLAN due to potential null pointer dereference while accessing the memory location in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	7.5	More Details
CVE-2022-45059	An issue was discovered in Varnish Cache 7.x before 7.1.2 and 7.2.x before 7.2.1. A request smuggling attack can be performed on Varnish Cache servers by requesting that certain headers are made hop-by-hop, preventing the Varnish Cache servers from forwarding critical headers to the backend.	7.5	More Details
CVE-2022-41058	Windows Network Address Translation (NAT) Denial of Service Vulnerability	7.5	More Details
CVE-2021-33159	Improper authentication in subsystem for Intel(R) AMT before versions 11.8.93, 11.22.93, 11.12.93, 12.0.92, 14.1.67, 15.0.42, 16.1.25 may allow a privileged user to potentially enable escalation of privilege via local access.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3972	A vulnerability was found in Pingkon HMS-PHP. It has been rated as critical. This issue affects some unknown processing of the file admin/adminlogin.php. The manipulation of the argument uname/pass leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-213551.	7.3	More Details
CVE-2022-3955	A vulnerability was found in tholum crm42. It has been rated as critical. This issue affects some unknown processing of the file crm42\class\class.user.php of the component Login. The manipulation of the argument user_name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-213461 was assigned to this vulnerability.	7.3	More Details
CVE-2022-29466	Improper input validation in firmware for Intel(R) SPS before version SPS_E3_04.01.04.700.0 may allow an authenticated user to potentially enable denial of service via local access.	7.3	More Details
CVE-2022-3265	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2. It was possible to exploit a vulnerability in setting the labels colour feature which could lead to a stored XSS that allowed attackers to perform arbitrary actions on behalf of victims at client side.	7.3	More Details
CVE-2022-3973	A vulnerability classified as critical has been found in Pingkon HMS-PHP. Affected is an unknown function of the file /admin/admin.php of the component Data Pump Metadata. The manipulation of the argument uname/pass leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-213552.	7.3	More Details
CVE-2022-33234	Memory corruption in video due to configuration weakness. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	7.3	More Details
CVE-2022-41878	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 5.3.2 or 4.10.19, keywords that are specified in the Parse Server option `requestKeywordDenylist` can be injected via Cloud Code Webhooks or Triggers. This will result in the keyword being saved to the database, bypassing the `requestKeywordDenylist` option. This issue is fixed in versions 4.10.19, and 5.3.2. If upgrade is not possible, the following Workarounds may be applied: Configure your firewall to only allow trusted servers to make request to the Parse Server Cloud Code Webhooks API, or block the API completely if you are not using the feature.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43030	Siyucms v6.1.7 was discovered to contain a remote code execution (RCE) vulnerability in the background. SIYUCMS is a content management system based on ThinkPaP5 AdminLTE. SIYUCMS has a background command execution vulnerability, which can be used by attackers to gain server privileges	7.2	More Details
CVE-2022-43292	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /youthappam/editfood.php.	7.2	More Details
CVE-2022-43278	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the categoriesId parameter at /php_action/fetchSelectedCategories.php.	7.2	More Details
CVE-2022-41879	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 5.3.3 or 4.10.20, a compromised Parse Server Cloud Code Webhook target endpoint allows an attacker to use prototype pollution to bypass the Parse Server `requestKeywordDenylist` option. This issue has been patched in versions 5.3.3 and 4.10.20. There are no known workarounds.	7.2	More Details
CVE-2022-43277	Canteen Management System v1.0 was discovered to contain an arbitrary file upload vulnerability via ip/youthappam/php_action/editFile.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-43146	An arbitrary file upload vulnerability in the image upload function of Canteen Management System v1.0 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-43279	LimeSurvey before v5.0.4 was discovered to contain a SQL injection vulnerability via the component /application/views/themeOptions/update.php.	7.2	More Details
CVE-2022-37967	Windows Kerberos Elevation of Privilege Vulnerability	7.2	More Details
CVE-2022-43290	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /youthappam/editcategory.php.	7.2	More Details
CVE-2022-45184	The Web Server in Ironman Software PowerShell Universal v3.x and v2.x allows for directory traversal outside of the configuration directory, which allows a remote attacker with administrator privilege to create, delete, update, and display files outside of the configuration directory via a crafted HTTP request to particular endpoints in the web server. Patched Versions are 3.5.3 and 3.4.7.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43291	Canteen Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /youthappam/editclient.php.	7.2	More Details
CVE-2022-38385	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.2.0 could allow an authenticated user to obtain highly sensitive information or perform unauthorized actions due to improper input validation. IBM X-Force ID: 233777.	7.1	More Details
CVE-2022-38387	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.2.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 233786.	7.1	More Details
CVE-2022-31253	A Untrusted Search Path vulnerability in openldap2 of openSUSE Factory allows local attackers with control of the ldap user or group to change ownership of arbitrary directory entries to this user/group, leading to escalation to root. This issue affects: openSUSE Factory openldap2 versions prior to 2.6.3-404.1.	7.1	More Details
CVE-2022-39880	Improper input validation vulnerability in DualOutFocusViewer prior to SMR Nov-2022 Release 1 allows local attacker to perform an arbitrary code execution.	7.1	More Details
CVE-2022-33908	DMA transactions which are targeted at input buffers used for the SdHostDriver software SMI handler could cause SMRAM corruption through a TOCTOU attack. DMA transactions which are targeted at input buffers used for the software SMI handler used by the SdHostDriver driver could cause SMRAM corruption through a TOCTOU attack. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. Fixed in kernel 5.2: 05.27.25, kernel 5.3: 05.36.25, kernel 5.4: 05.44.25, kernel 5.5: 05.52.25 https://www.insyde.com/security-pledge/SA-2022050	7.0	More Details
CVE-2022-41114	Windows Bind Filter Driver Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-33905	DMA transactions which are targeted at input buffers used for the AhciBusDxe software SMI handler could cause SMRAM corruption (a TOCTOU attack). DMA transactions which are targeted at input buffers used for the software SMI handler used by the AhciBusDxe driver could cause SMRAM corruption through a TOCTOU attack. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group, Fixed in kernel 5.2: 05.27.23, kernel 5.3: 05.36.23, kernel 5.4: 05.44.23, kernel 5.5: 05.52.23 https://www.insyde.com/security-pledge/SA-2022047	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33985	DMA transactions which are targeted at input buffers used for the NvmExpressDxe software SMI handler could cause SMRAM corruption through a TOCTOU attack. DMA transactions which are targeted at input buffers used for the software SMI handler used by the NvmExpressDxe driver could cause SMRAM corruption through a TOCTOU attack. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. This issue was fixed in kernel 5.2: 05.27.25, kernel 5.3: 05.36.25, kernel 5.4: 05.44.25, kernel 5.5: 05.52.25 https://www.insyde.com/security-pledge/SA-2022055	7.0	More Details
CVE-2022-33984	DMA transactions which are targeted at input buffers used for the SdMmcDevice software SMI handler could cause SMRAM corruption through a TOCTOU attack. DMA transactions which are targeted at input buffers used for the software SMI handler used by the SdMmcDevice driver could cause SMRAM corruption through a TOCTOU attack. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. This was fixed in kernel 5.2: 05.27.25, kernel 5.3: 05.36.25, kernel 5.4: 05.44.25, kernel 5.5: 05.52.25 https://www.insyde.com/security-pledge/SA-2022054	7.0	More Details
CVE-2022-33983	DMA transactions which are targeted at input buffers used for the NvmExpressLegacy software SMI handler could cause SMRAM corruption through a TOCTOU attack. DMA transactions which are targeted at input buffers used for the software SMI handler used by the NvmExpressLegacy driver could cause SMRAM corruption through a TOCTOU attack. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. This issue was fixed in kernel 5.2: 05.27.25, kernel 5.3: 05.36.25, kernel 5.4: 05.44.25, kernel 5.5: 05.52.25 https://www.insyde.com/security-pledge/SA-2022053	7.0	More Details
CVE-2022-33909	DMA transactions which are targeted at input buffers used for the HddPassword software SMI handler could cause SMRAM corruption through a TOCTOU attack. DMA transactions which are targeted at input buffers used for the software SMI handler used by the HddPassword driver could cause SMRAM corruption through a TOCTOU attack..This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. Fixed in kernel Kernel 5.2: 05.27.23, Kernel 5.3: 05.36.23, Kernel 5.4: 05.44.23, Kernel 5.5: 05.52.23 https://www.insyde.com/security-pledge/SA-2022051	7.0	More Details
CVE-2022-38014	Windows Subsystem for Linux (WSL2) Kernel Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25676	Information disclosure in video due to buffer over-read while parsing avi files in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	6.8	More Details
CVE-2022-28611	Improper input validation in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2022-27874	Improper authentication in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via physical access.	6.8	More Details
CVE-2022-26024	Improper access control in the Intel(R) NUC HDMI Firmware Update Tool for NUC7i3DN, NUC7i5DN and NUC7i7DN before version 1.78.2.0.7 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-36384	Unquoted search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-26028	Uncontrolled search path in the Intel(R) VTune(TM) Profiler software before version 2022.2.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-33064	Uncontrolled search path in the software installer for Intel(R) System Studio for all versions, may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-27638	Uncontrolled search path element in the Intel(R) Advanced Link Analyzer Pro before version 22.2 and Standard edition software before version 22.1.1 STD may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-0031	A local privilege escalation (PE) vulnerability in the Palo Alto Networks Cortex XSOAR engine software running on a Linux operating system allows a local attacker with shell access to the engine to execute programs with elevated privileges.	6.7	More Details
CVE-2022-36377	Insecure inherited permissions in some Intel(R) Wireless Adapter Driver installation software for Intel(R) NUC Kits & Mini PCs before version 22.190.0.3 for Windows may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36380	Uncontrolled search path in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-27187	Uncontrolled search path element in the Intel(R) Quartus Prime Standard edition software before version 21.1 Patch 0.02std may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-36400	Path traversal in the installer software for some Intel(r) NUC Kit Wireless Adapter drivers for Windows 10 before version 22.40 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-26086	Uncontrolled search path element in the PresentMon software maintained by Intel(R) before version 1.7.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-30548	Uncontrolled search path element in the Intel(R) Glorp software may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-39307	Grafana is an open-source platform for monitoring and observability. When using the forget password on the login page, a POST request is made to the `/api/user/password/sent-reset-email` URL. When the username or email does not exist, a JSON response contains a “user not found” message. This leaks information to unauthenticated users and introduces a security risk. This issue has been patched in 9.2.4 and backported to 8.5.15. There are no known workarounds.	6.7	More Details
CVE-2022-44244	An authentication bypass in Lin-CMS v0.2.1 allows attackers to escalate privileges to Super Administrator.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41882	The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server with your computer. In version 3.6.0, if a user received a malicious file share and has it synced locally or the virtual filesystem enabled and clicked a nc://open/ link it will open the default editor for the file type of the shared file, which on Windows can also sometimes mean that a file depending on the type, e.g. "vbs", is being executed. It is recommended that the Nextcloud Desktop client is upgraded to version 3.6.1. As a workaround, users can block the Nextcloud Desktop client 3.6.0 by setting the `minimum.supported.desktop.version` system config to `3.6.1` on the server, so new files designed to use this attack vector are not downloaded anymore. Already existing files can still be used. Another workaround would be to enforce shares to be accepted by setting the `sharing.force_share_accept` system config to `true` on the server, so new files designed to use this attack vector are not downloaded anymore. Already existing shares can still be abused.	6.6	More Details
CVE-2022-43686	In Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2, the authTypeConcreteCookieMap table can be filled up causing a denial of service (high load).	6.5	More Details
CVE-2022-45383	An incorrect permission check in Jenkins Support Core Plugin 1206.v14049fa_b_d860 and earlier allows attackers with Support/DownloadBundle permission to download a previously created support bundle containing information limited to users with Overall/Administer permission.	6.5	More Details
CVE-2022-25674	Cryptographic issues in WLAN during the group key handshake of the WPA/WPA2 protocol in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music	6.5	More Details
CVE-2022-31630	In PHP versions prior to 7.4.33, 8.0.25 and 8.1.12, when using imageloadfont() function in gd extension, it is possible to supply a specially crafted font file, such as if the loaded font is used with imagechar() function, the read outside allocated buffer will be used. This can lead to crashes or disclosure of confidential information.	6.5	More Details
CVE-2022-38015	Windows Hyper-V Denial of Service Vulnerability	6.5	More Details
CVE-2022-40845	The Tenda AC1200 Router model W15Ev2 V15.11.0.10(1576) is affected by a password exposure vulnerability. When combined with the improper authorization/improper session management vulnerability, an attacker with access to the router may be able to expose sensitive information which they're not explicitly authorized to have.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45130	Plesk Obsidian allows a CSRF attack, e.g., via the /api/v2/cli/commands REST API to change an Admin password. NOTE: Obsidian is a specific version of the Plesk product: version numbers were used through version 12, and then the convention was changed so that versions are identified by names ("Obsidian"), not numbers.	6.5	More Details
CVE-2022-38120	UPSMON PRO's has a path traversal vulnerability. A remote attacker with general user privilege can exploit this vulnerability to bypass authentication and access arbitrary system files.	6.5	More Details
CVE-2022-38121	UPSMON PRO configuration file stores user password in plaintext under public user directory. A remote attacker with general user privilege can access all users‘ and administrators' account names and passwords via this unprotected configuration file.	6.5	More Details
CVE-2022-34666	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a local user with basic capabilities can cause a null-pointer dereference, which may lead to denial of service.	6.5	More Details
CVE-2022-41122	Microsoft SharePoint Server Spoofing Vulnerability	6.5	More Details
CVE-2022-3632	The OAuth Client by DigitialPixies WordPress plugin through 1.1.0 does not have CSRF checks in some places, which could allow attackers to make logged-in users perform unwanted actions.	6.5	More Details
CVE-2022-27233	XML injection in the Quartus(R) Prime Programmer included in the Intel(R) Quartus Prime Pro and Standard edition software may allow an unauthenticated user to potentially enable information disclosure via network access.	6.5	More Details
CVE-2022-41097	Network Policy Server (NPS) RADIUS Protocol Information Disclosure Vulnerability	6.5	More Details
CVE-2022-44389	EyouCMS V1.5.9-UTF8-SP1 was discovered to contain a Cross-Site Request Forgery (CSRF) via the Edit Admin Profile module. This vulnerability allows attackers to arbitrarily change Administrator account information.	6.5	More Details
CVE-2022-45392	Jenkins NS-ND Integration Performance Publisher Plugin 4.8.0.143 and earlier stores passwords unencrypted in job config.xml files on the Jenkins controller where they can be viewed by attackers with Extended Read permission, or access to the Jenkins controller file system.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45384	Jenkins Reverse Proxy Auth Plugin 1.7.3 and earlier stores the LDAP manager password unencrypted in the global config.xml file on the Jenkins controller where it can be viewed by attackers with access to the Jenkins controller file system.	6.5	More Details
CVE-2022-24938	A malformed packet causes a stack overflow in the Ember ZNet stack. This causes an assert which leads to a reset, immediately clearing the error.	6.5	More Details
CVE-2022-24937	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in Silicon Labs Ember ZNet allows Overflow Buffers.	6.5	More Details
CVE-2022-42460	Broken Access Control vulnerability leading to Stored Cross-Site Scripting (XSS) in Traffic Manager plugin <= 1.4.5 on WordPress.	6.5	More Details
CVE-2022-29481	A leftover debug code vulnerability exists in the console nvram functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted series of network requests can lead to disabling security features. An attacker can send a sequence of requests to trigger this vulnerability.	6.5	More Details
CVE-2022-26023	A leftover debug code vulnerability exists in the console verify functionality of InHand Networks InRouter302 V3.5.45. A specially-crafted series of network requests can lead to disabling security features. An attacker can send a sequence of requests to trigger this vulnerability.	6.5	More Details
CVE-2022-2449	The reSmush.it : the only free Image Optimizer & compress plugin WordPress plugin before 0.4.4 does not perform CSRF checks for any of its AJAX actions, allowing an attackers to trick logged in users to perform various actions on their behalf on the site.	6.5	More Details
CVE-2021-34577	In the Kaden PICOFLUX AiR water meter an adversary can read the values through wireless M-Bus mode 5 with a hardcoded shared key while being adjacent to the device.	6.5	More Details
CVE-2022-39385	Discourse is the an open source discussion platform. In some rare cases users redeeming an invitation can be added as a participant to several private message topics that they should not be added to. They are not notified of this, it happens transparently in the background. This issue has been resolved in commit `a414520742` and will be included in future releases. Users are advised to upgrade. Users are also advised to set `SiteSetting.max_invites_per_day` to 0 until the patch is installed.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40225	A vulnerability has been identified in SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0) (All versions < V2.4.8), TIM 1531 IRC (6GK7543-1MX00-0XE0) (All versions < V2.4.8). Casting an internal value could lead to floating point exception under certain circumstances. This could allow an attacker to cause a denial of service condition on affected devices.	6.5	More Details
CVE-2022-40903	Aiphone GT-DMB-N 3-in-1 Video Entrance Station with NFC Reader 1.0.3 does not mitigate against repeated failed access attempts, which allows an attacker to gain administrative privileges.	6.5	More Details
CVE-2022-28667	Out-of-bounds write for some Intel(R) PROSet/Wireless WiFi software before version 22.140 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2022-20949	A vulnerability in the management web server of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker with high privileges to execute configuration commands on an affected system. This vulnerability exists because access to HTTPS endpoints is not properly restricted on an affected device. An attacker could exploit this vulnerability by sending specific messages to the affected HTTPS handler. A successful exploit could allow the attacker to perform configuration changes on the affected system, which should be configured and managed only through Cisco Firepower Management Center (FMC) Software.	6.5	More Details
CVE-2022-3538	The Webmaster Tools Verification WordPress plugin through 1.2 does not have authorisation and CSRF checks when disabling plugins, allowing unauthenticated users to disable arbitrary plugins	6.5	More Details
CVE-2022-41086	Windows Group Policy Elevation of Privilege Vulnerability	6.4	More Details
CVE-2022-39306	Grafana is an open-source platform for monitoring and observability. Versions prior to 9.2.4, or 8.5.15 on the 8.X branch, are subject to Improper Input Validation. Grafana admins can invite other members to the organization they are an admin for. When admins add members to the organization, non existing users get an email invite, existing members are added directly to the organization. When an invite link is sent, it allows users to sign up with whatever username/email address the user chooses and become a member of the organization. This introduces a vulnerability which can be used with malicious intent. This issue is patched in version 9.2.4, and has been backported to 8.5.15. There are no known workarounds.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41904	Element iOS is an iOS Matrix client provided by Element. It is based on MatrixSDK. Prior to version 1.9.7, events encrypted using Megolm for which trust could not be established did not get decorated accordingly (with warning shields). Therefore a malicious homeserver could inject messages into the room without the user being alerted that the messages were not sent by a verified group member, even if the user has previously verified all group members. This issue has been patched in Element iOS 1.9.7. There are currently no known workarounds.	6.4	More Details
CVE-2022-20826	A vulnerability in the secure boot implementation of Cisco Secure Firewalls 3100 Series that are running Cisco Adaptive Security Appliance (ASA) Software or Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated attacker with physical access to the device to bypass the secure boot functionality. This vulnerability is due to a logic error in the boot process. An attacker could exploit this vulnerability by injecting malicious code into a specific memory location during the boot process of an affected device. A successful exploit could allow the attacker to execute persistent code at boot time and break the chain of trust.	6.4	More Details
CVE-2022-30773	DMA attacks on the parameter buffer used by the IhisiSmm driver could change the contents after parameter values have been checked but before they are used (a TOCTOU attack). DMA attacks on the parameter buffer used by the IhisiSmm driver could change the contents after parameter values have been checked but before they are used (a TOCTOU attack). This issue was discovered by Insyde engineering. This issue is fixed in Kernel 5.4: 05.44.23 and Kernel 5.5: 05.52.23. CWE-367	6.4	More Details
CVE-2022-33986	DMA attacks on the parameter buffer used by the VariableRuntimeDxe software SMI handler could lead to a TOCTOU attack. DMA attacks on the parameter buffer used by the software SMI handler used by the driver VariableRuntimeDxe could lead to a TOCTOU attack on the SMI handler and lead to corruption of SMRAM. This issue was discovered by Insyde engineering during a security review. This issue is fixed in Kernel 5.4: 05.44.23 and Kernel 5.5: 05.52.23. CWE-367 CWE-367 Report at: https://www.insyde.com/security-pledge/SA-2022056	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32266	DMA attacks on the parameter buffer used by a software SMI handler used by the driver PcdSmmDxe could lead to a TOCTOU attack on the SMI handler and lead to corruption of other ACPI fields and adjacent memory fields. DMA attacks on the parameter buffer used by a software SMI handler used by the driver PcdSmmDxe could lead to a TOCTOU attack on the SMI handler and lead to corruption of other ACPI fields and adjacent memory fields. The attack would require detailed knowledge of the PCD database contents on the current platform. This issue was discovered by Insyde engineering during a security review. This issue is fixed in Kernel 5.3: 05.36.23, Kernel 5.4: 05.44.23, Kernel 5.5: 05.52.23. Kernel 5.2 is unaffected. CWE-787 An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. DMA attacks on the parameter buffer that is used by a software SMI handler (used by the PcdSmmDxe driver) could lead to a TOCTOU race-condition attack on the SMI handler, and lead to corruption of other ACPI fields and adjacent memory fields. The attack would require detailed knowledge of the PCD database contents on the current platform.	6.4	More Details
CVE-2022-33906	DMA transactions which are targeted at input buffers used for the FwBlockServiceSmm software SMI handler could cause SMRAM corruption through a TOCTOU attack. DMA transactions which are targeted at input buffers used for the software SMI handler used by the FwBlockServiceSmm driver could cause SMRAM corruption through a TOCTOU attack. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. Fixed in kernel 5.2: 05.27.23, 5.3: 05.36.23, 5.4: 05.44.23, 5.5: 05.52.23 https://www.insyde.com/security-pledge/SA-2022048	6.4	More Details
CVE-2022-32267	DMA transactions which are targeted at input buffers used for the SmmResourceCheckDxe software SMI handler cause SMRAM corruption (a TOCTOU attack) DMA transactions which are targeted at input buffers used for the software SMI handler used by the SmmResourceCheckDxe driver could cause SMRAM corruption through a TOCTOU attack... This issue was discovered by Insyde engineering. Fixed in kernel Kernel 5.2: 05.27.23. Kernel 5.3: 05.36.23. Kernel 5.4: 05.44.23. Kernel 5.5: 05.52.23 https://www.insyde.com/security-pledge/SA-2022046	6.4	More Details
CVE-2022-31243	Update description and links DMA transactions which are targeted at input buffers used for the software SMI handler used by the FvbServicesRuntimeDxe driver could cause SMRAM corruption through a TOCTOU attack.. "DMA transactions which are targeted at input buffers used for the software SMI handler used by the FvbServicesRuntimeDxe driver could cause SMRAM corruption. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. Fixed in Kernel 5.2: 05.27.21. Kernel 5.3: 05.36.21. Kernel 5.4: 05.44.21. Kernel 5.5: 05.52.21 https://www.insyde.com/security-pledge/SA-2022044	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30774	DMA attacks on the parameter buffer used by the PnpSmm driver could change the contents after parameter values have been checked but before they are used (a TOCTOU attack) DMA attacks on the parameter buffer used by the PnpSmm driver could change the contents after parameter values have been checked but before they are used (a TOCTOU attack) . This issue was discovered by Insyde engineering during a security review. This iss was fixed in Kernel 5.2: 05.27.29, Kernel 5.3: 05.36.25, Kernel 5.4: 05.44.25, Kernel 5.5: 05.52.25. CWE-367 https://www.insyde.com/security-pledge/SA-2022043	6.4	More Details
CVE-2022-33982	DMA attacks on the parameter buffer used by the Int15ServiceSmm software SMI handler could lead to a TOCTOU attack on the SMI handler and lead to corruption of SMRAM. DMA attacks on the parameter buffer used by the software SMI handler used by the driver Int15ServiceSmm could lead to a TOCTOU attack on the SMI handler and lead to corruption of SMRAM. This issue was discovered by Insyde engineering during a security review. This issue is fixed in Kernel 5.2: 05.27.23, Kernel 5.3: 05.36.23, Kernel 5.4: 05.44.23 and Kernel 5.5: 05.52.23 CWE-367	6.4	More Details
CVE-2022-33907	DMA transactions which are targeted at input buffers used for the software SMI handler used by the IdeBusDxe driver could cause SMRAM corruption through a TOCTOU attack... DMA transactions which are targeted at input buffers used for the software SMI handler used by the IdeBusDxe driver could cause SMRAM corruption through a TOCTOU attack. This issue was discovered by Insyde engineering based on the general description provided by Intel's iSTARE group. Fixed in kernel 5.2: 05.27.25, kernel 5.3: 05.36.25, kernel 5.4: 05.44.25 https://www.insyde.com/security-pledge/SA-2022049	6.4	More Details
CVE-2022-20925	A vulnerability in the web management interface of the Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. The vulnerability is due to insufficient validation of user-supplied parameters for certain API endpoints. An attacker could exploit this vulnerability by sending crafted input to an affected API endpoint. A successful exploit could allow an attacker to execute arbitrary commands on the device with low system privileges. To successfully exploit this vulnerability, an attacker would need valid credentials for a user with Device permissions: by default, only Administrators, Security Approvers and Network Admins user accounts have these permissions.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20926	A vulnerability in the web management interface of the Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. The vulnerability is due to insufficient validation of user-supplied parameters for certain API endpoints. An attacker could exploit this vulnerability by sending crafted input to an affected API endpoint. A successful exploit could allow an attacker to execute arbitrary commands on the device with low system privileges. To successfully exploit this vulnerability, an attacker would need valid credentials for a user with Device permissions: by default, only Administrators, Security Approvers and Network Admins user accounts have these permissions.	6.3	More Details
CVE-2022-3974	A vulnerability classified as critical was found in Axiomatic Bento4. Affected by this vulnerability is the function AP4_StdcFileByteStream::ReadPartial of the file Ap4StdCFileByteStream.cpp of the component mp4info. The manipulation leads to heap-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-213553 was assigned to this vulnerability.	6.3	More Details
CVE-2022-43690	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 did not use strict comparison for the legacy_salt so that limited authentication bypass could occur if using this functionality. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+.	6.3	More Details
CVE-2022-3970	A vulnerability was found in LibTIFF. It has been classified as critical. This affects the function TIFFReadRGBATileExt of the file libtiff/tif_getimage.c. The manipulation leads to integer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 227500897dfb07fb7d27f7aa570050e62617e3be. It is recommended to apply a patch to fix this issue. The identifier VDB-213549 was assigned to this vulnerability.	6.3	More Details
CVE-2022-3997	A vulnerability, which was classified as critical, has been found in MonikaBrzica scm. Affected by this issue is some unknown functionality of the file upis_u_bazu.php. The manipulation of the argument email/lozinka/ime/id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-213698 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-3998	A vulnerability, which was classified as critical, was found in MonikaBrzica scm. This affects an unknown part of the file uredi_korisnika.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-213699.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41918	OpenSearch is a community-driven, open source fork of Elasticsearch and Kibana. There is an issue with the implementation of fine-grained access control rules (document-level security, field-level security and field masking) where they are not correctly applied to the indices that back data streams potentially leading to incorrect access authorization. OpenSearch 1.3.7 and 2.4.0 contain a fix for this issue. Users are advised to update. There are no known workarounds for this issue.	6.3	More Details
CVE-2022-3939	A vulnerability, which was classified as critical, has been found in lanyulei ferry. Affected by this issue is some unknown functionality of the file apis/public/file.go of the component API. The manipulation of the argument file leads to path traversal. The attack may be launched remotely. VDB-213446 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-3947	A vulnerability classified as critical has been found in eolinker goku_lite. This affects an unknown part of the file /balance/service/list. The manipulation of the argument route/keyword leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-213453 was assigned to this vulnerability.	6.3	More Details
CVE-2022-3956	A vulnerability classified as critical has been found in tsruban HHIMS 2.1. Affected is an unknown function of the component Patient Portrait Handler. The manipulation of the argument PID leads to sql injection. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue. VDB-213462 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-3948	A vulnerability classified as critical was found in eolinker goku_lite. This vulnerability affects unknown code of the file /plugin/getList. The manipulation of the argument route/keyword leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-213454 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-3944	A vulnerability was found in jerryhanjj ERP. It has been declared as critical. Affected by this vulnerability is the function uploadImages of the file application/controllers/basedata/inventory.php of the component Commodity Management. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-213451.	6.3	More Details
CVE-2022-41607	All versions of ETIC Telecom Remote Access Server (RAS) 4.5.0 and prior's application programmable interface (API) is vulnerable to directory traversal through several different methods. This could allow an attacker to read sensitive files from the server, including SSH private keys, passwords, scripts, python objects, database files, and more.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39890	Improper Authorization in Samsung Billing prior to version 5.0.56.0 allows attacker to get sensitive information.	6.2	More Details
CVE-2022-25679	Denial of service in video due to improper access control in broadcast receivers in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	6.2	More Details
CVE-2022-26369	Out-of-bounds read in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via adjacent access.	6.2	More Details
CVE-2022-31688	VMware Workspace ONE Assist prior to 22.10 contains a Reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window.	6.1	More Details
CVE-2022-35740	dotCMS before 22.06 allows remote attackers to bypass intended access control and obtain sensitive information by using a semicolon in a URL to introduce a matrix parameter. (This is also fixed in 5.3.8.12, 21.06.9, and 22.03.2 for LTS users.) Some Java application frameworks, including those used by Spring or Tomcat, allow the use of matrix parameters: these are URI parameters separated by semicolons. Through precise semicolon placement in a URI, it is possible to exploit this feature to avoid dotCMS's path-based XSS prevention (such as "require login" filters), and consequently access restricted resources. For example, an attacker could place a semicolon immediately before a / character that separates elements of a filesystem path. This could reveal file content that is ordinarily only visible to signed-in users. This issue can be chained with other exploit code to achieve XSS attacks against dotCMS.	6.1	More Details
CVE-2021-40272	OP5 Monitor 8.3.1, 8.3.2, and OP5 8.3.3 are vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2022-43692	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Reflected XSS - user can cause an administrator to trigger reflected XSS with a url if the targeted administrator is using an old browser that lacks XSS protection. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+.	6.1	More Details
CVE-2022-3415	The Chat Bubble WordPress plugin before 2.3 does not sanitise and escape some contact parameters, which could allow unauthenticated attackers to set Stored Cross-Site Scripting payloads in them, which will trigger when an admin view the related contact message	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3484	The WPB Show Core WordPress plugin does not sanitize and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-38201	An unvalidated redirect vulnerability exists in Esri Portal for ArcGIS Quick Capture Web Designer versions 10.8.1 to 10.9.1. A remote, unauthenticated attacker can potentially induce an unsuspecting authenticated user to access an an attacker controlled domain.	6.1	More Details
CVE-2021-40289	mm-wki v0.2.1 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2022-43694	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Reflected XSS in the image manipulation library due to un-sanitized output.	6.1	More Details
CVE-2022-42110	A Cross-site scripting (XSS) vulnerability in the Announcements module in Liferay Portal 7.1.0 through 7.4.2, and Liferay DXP 7.1 before fix pack 27, 7.2 before fix pack 17, and 7.3 before service pack 3 allows remote attackers to inject arbitrary web script or HTML.	6.1	More Details
CVE-2022-42118	A Cross-site scripting (XSS) vulnerability in the Portal Search module in Liferay Portal 7.1.0 through 7.4.2, and Liferay DXP 7.1 before fix pack 27, 7.2 before fix pack 15, and 7.3 before service pack 3 allows remote attackers to inject arbitrary web script or HTML via the `tag` parameter.	6.1	More Details
CVE-2022-43121	A cross-site scripting (XSS) vulnerability in the CMS Field Add page of Intelliants Subrion CMS v4.2.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the tooltip text field.	6.1	More Details
CVE-2022-38167	The Nintex Workflow plugin 5.2.2.30 for SharePoint allows XSS.	6.1	More Details
CVE-2022-43967	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Reflected XSS in the multilingual report due to un-sanitized output. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+.	6.1	More Details
CVE-2022-43120	A cross-site scripting (XSS) vulnerability in the /panel/fields/add component of Intelliants Subrion CMS v4.2.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Field default value text field.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43968	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Reflected XSS in the dashboard icons due to un-sanitized output. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+.	6.1	More Details
CVE-2022-43119	A cross-site scripting (XSS) vulnerability in Clansphere CMS v2011.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Username parameter.	6.1	More Details
CVE-2022-43118	A cross-site scripting (XSS) vulnerability in flatCore-CMS v2.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Username text field.	6.1	More Details
CVE-2022-43321	Shopwind v3.4.3 was discovered to contain a reflected cross-site scripting (XSS) vulnerability in the component /common/library/Page.php.	6.1	More Details
CVE-2022-43320	FeehiCMS v2.1.1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the id parameter at /web/admin/index.php?r=log%2Fview-layer.	6.1	More Details
CVE-2022-45402	In Apache Airflow versions prior to 2.4.3, there was an open redirect in the webserver's `/login` endpoint.	6.1	More Details
CVE-2022-3578	The ProfileGrid WordPress plugin before 5.1.1 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-25917	Uncaught exception in the firmware for some Intel(R) Server Board M50CYP Family before version R01.01.0005 may allow a privileged user to potentially enable a denial of service via local access.	6.0	More Details
CVE-2022-26367	Improper buffer restrictions in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via local access.	6.0	More Details
CVE-2022-28126	Improper input validation in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via local access.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20934	A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software and Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system as root. This vulnerability is due to improper input validation for specific CLI commands. An attacker could exploit this vulnerability by injecting operating system commands into a legitimate command. A successful exploit could allow the attacker to escape the restricted command prompt and execute arbitrary commands on the underlying operating system. To successfully exploit this vulnerability, an attacker would need valid Administrator credentials.	6.0	More Details
CVE-2022-26079	Improper conditions check in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via local access.	6.0	More Details
CVE-2022-29515	Missing release of memory after effective lifetime in firmware for Intel(R) SPS before versions SPS_E3_06.00.03.035.0 may allow a privileged user to potentially enable denial of service via local access.	6.0	More Details
CVE-2022-42964	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the pymatgen PyPI package, when an attacker is able to supply arbitrary input to the GaussianInput.from_string method	5.9	More Details
CVE-2022-41916	Heimdal is an implementation of ASN.1/DER, PKIX, and Kerberos. Versions prior to 7.7.1 are vulnerable to a denial of service vulnerability in Heimdal's PKI certificate validation library, affecting the KDC (via PKINIT) and kinit (via PKINIT), as well as any third-party applications using Heimdal's libhx509. Users should upgrade to Heimdal 7.7.1 or 7.8. There are no known workarounds for this issue.	5.9	More Details
CVE-2022-45193	CBRN-Analysis before 22 has weak file permissions under Public Profile, leading to disclosure of file contents or privilege escalation.	5.9	More Details
CVE-2022-41116	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability	5.9	More Details
CVE-2022-39886	Improper access control vulnerability in IpcRxServiceModeBigDataInfo in RIL prior to SMR Nov-2022 Release 1 allows local attacker to access Device information.	5.9	More Details
CVE-2022-39885	Improper access control vulnerability in BootCompletedReceiver_CMCC in DeviceManagement prior to SMR Nov-2022 Release 1 allows local attacker to access to Device information.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41090	Windows Point-to-Point Tunneling Protocol Denial of Service Vulnerability	5.9	More Details
CVE-2022-42132	The Test LDAP Users functionality in Liferay Portal 7.0.0 through 7.4.3.4, and Liferay DXP 7.0 fix pack 102 and earlier, 7.1 before fix pack 27, 7.2 before fix pack 17, 7.3 before update 4, and DXP 7.4 GA includes the LDAP credential in the page URL when paginating through the list of users, which allows man-in-the-middle attackers or attackers with access to the request logs to see the LDAP credential.	5.9	More Details
CVE-2022-34320	IBM CICS TX 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 229464.	5.9	More Details
CVE-2022-39879	Improper authorization vulnerability in?CallBGProvider prior to SMR Nov-2022 Release 1 allows local attacker to grant permission for accessing information with phone uid.	5.9	More Details
CVE-2022-44563	There is a race condition vulnerability in SD upgrade mode. Successful exploitation of this vulnerability may affect data confidentiality.	5.9	More Details
CVE-2022-34319	IBM CICS TX 11.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 229463.	5.9	More Details
CVE-2022-40981	All versions of ETIC Telecom Remote Access Server (RAS) 4.5.0 and prior is vulnerable to malicious file upload. An attacker could take advantage of this to store malicious files on the server, which could override sensitive and useful existing files on the filesystem, fill the hard disk to full capacity, or compromise the affected device or computers with administrator level privileges connected to the affected device.	5.9	More Details
CVE-2022-30691	Uncontrolled resource consumption in the Intel(R) Support Android application before version 22.02.28 may allow an authenticated user to potentially enable denial of service via local access.	5.9	More Details
CVE-2022-42966	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the cleo PyPI package, when an attacker is able to supply arbitrary input to the Table.set_rows method	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39392	Wasmtime is a standalone runtime for WebAssembly. Prior to version 2.0.2, there is a bug in Wasmtime's implementation of its pooling instance allocator when the allocator is configured to give WebAssembly instances a maximum of zero pages of memory. In this configuration, the virtual memory mapping for WebAssembly memories did not meet the compiler-required configuration requirements for safely executing WebAssembly modules. Wasmtime's default settings require virtual memory page faults to indicate that wasm reads/writes are out-of-bounds, but the pooling allocator's configuration would not create an appropriate virtual memory mapping for this meaning out of bounds reads/writes can successfully read/write memory unrelated to the wasm sandbox within range of the base address of the memory mapping created by the pooling allocator. This bug is not applicable with the default settings of the `wasmtime` crate. This bug can only be triggered by setting `InstanceLimits::memory_pages` to zero. This is expected to be a very rare configuration since this means that wasm modules cannot allocate any pages of linear memory. All wasm modules produced by all current toolchains are highly likely to use linear memory, so it's expected to be unlikely that this configuration is set to zero by any production embedding of Wasmtime. This bug has been patched and users should upgrade to Wasmtime 2.0.2. This bug can be worked around by increasing the `memory_pages` allotment when configuring the pooling allocator to a value greater than zero. If an embedding wishes to still prevent memory from actually being used then the `Store::limiter` method can be used to dynamically disallow growth of memory beyond 0 bytes large. Note that the default `memory_pages` value is greater than zero.	5.9	More Details
CVE-2022-20922	Multiple vulnerabilities in the Server Message Block Version 2 (SMB2) processor of the Snort detection engine on multiple Cisco products could allow an unauthenticated, remote attacker to bypass the configured policies or cause a denial of service (DoS) condition on an affected device. These vulnerabilities are due to improper management of system resources when the Snort detection engine is processing SMB2 traffic. An attacker could exploit these vulnerabilities by sending a high rate of certain types of SMB2 packets through an affected device. A successful exploit could allow the attacker to trigger a reload of the Snort process, resulting in a DoS condition. Note: When the snort preserve-connection option is enabled for the Snort detection engine, a successful exploit could also allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network. The snort preserve-connection setting is enabled by default. See the Details ["#details"] section of this advisory for more information. Note: Only products that have Snort 3 configured are affected. Products that are configured with Snort 2 are not affected.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20943	Multiple vulnerabilities in the Server Message Block Version 2 (SMB2) processor of the Snort detection engine on multiple Cisco products could allow an unauthenticated, remote attacker to bypass the configured policies or cause a denial of service (DoS) condition on an affected device. These vulnerabilities are due to improper management of system resources when the Snort detection engine is processing SMB2 traffic. An attacker could exploit these vulnerabilities by sending a high rate of certain types of SMB2 packets through an affected device. A successful exploit could allow the attacker to trigger a reload of the Snort process, resulting in a DoS condition. Note: When the snort preserve-connection option is enabled for the Snort detection engine, a successful exploit could also allow the attacker to bypass the configured policies and deliver a malicious payload to the protected network. The snort preserve-connection setting is enabled by default. See the Details ["#details"] section of this advisory for more information. Note: Only products that have Snort 3 configured are affected. Products that are configured with Snort 2 are not affected.	5.8	More Details
CVE-2022-41854	Those using Snakeyaml to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stack overflow. This effect may support a denial of service attack.	5.8	More Details
CVE-2022-41064	.NET Framework Information Disclosure Vulnerability	5.8	More Details
CVE-2022-20928	A vulnerability in the authentication and authorization flows for VPN connections in Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to establish a connection as a different user. This vulnerability is due to a flaw in the authorization verifications during the VPN authentication flow. An attacker could exploit this vulnerability by sending a crafted packet during a VPN authentication. The attacker must have valid credentials to establish a VPN connection. A successful exploit could allow the attacker to establish a VPN connection with access privileges from a different user.	5.8	More Details
CVE-2022-20950	A vulnerability in the interaction of SIP and Snort 3 for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the Snort 3 detection engine to restart. This vulnerability is due to a lack of error-checking when SIP bidirectional flows are being inspected by Snort 3. An attacker could exploit this vulnerability by sending a stream of crafted SIP traffic through an interface on the targeted device. A successful exploit could allow the attacker to trigger a restart of the Snort 3 process, resulting in a denial of service (DoS) condition.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3979	A vulnerability was found in NagVis up to 1.9.33 and classified as problematic. This issue affects the function checkAuthCookie of the file share/server/core/classes/CoreLogonMultisite.php. The manipulation of the argument hash leads to incorrect type conversion. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. Upgrading to version 1.9.34 is able to address this issue. The identifier of the patch is 7574fd8a2903282c2e0d1feef5c4876763db21d5. It is recommended to upgrade the affected component. The identifier VDB-213557 was assigned to this vulnerability.	5.6	More Details
CVE-2022-41055	Windows Human Interface Device Information Disclosure Vulnerability	5.5	More Details
CVE-2022-41060	Microsoft Word Information Disclosure Vulnerability	5.5	More Details
CVE-2022-43071	A stack overflow in the Catalog::readPageLabelTree2(Object*) function of XPDF v4.04 allows attackers to cause a Denial of Service (DoS) via a crafted PDF file.	5.5	More Details
CVE-2022-23824	IBPB may not prevent return branch predictions from being specified by pre-IBPB branch targets leading to a potential information disclosure.	5.5	More Details
CVE-2022-43295	XPDF v4.04 was discovered to contain a stack overflow via the function FileStream::copy() at xpdf/Stream.cc:795.	5.5	More Details
CVE-2022-45386	Jenkins Violations Plugin 0.7.11 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	5.5	More Details
CVE-2022-41105	Microsoft Excel Information Disclosure Vulnerability	5.5	More Details
CVE-2021-26393	Insufficient memory cleanup in the AMD Secure Processor (ASP) Trusted Execution Environment (TEE) may allow an authenticated attacker with privileges to generate a valid signed TA and potentially poison the contents of the process memory with attacker controlled data resulting in a loss of confidentiality.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3976	A vulnerability has been found in MZ Automation libiec61850 up to 1.4 and classified as critical. This vulnerability affects unknown code of the file src/mms/iso_mms/client/mms_client_files.c of the component MMS File Services. The manipulation of the argument filename leads to path traversal. Upgrading to version 1.5 is able to address this issue. The name of the patch is 10622ba36bb3910c151348f1569f039ecdd8786f. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-213556.	5.5	More Details
CVE-2022-3483	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.1 before 15.3.5, all versions starting from 15.4 before 15.4.4, all versions starting from 15.5 before 15.5.2. A malicious maintainer could exfiltrate a Datadog integration's access token by modifying the integration URL such that authenticated requests are sent to an attacker controlled server.	5.5	More Details
CVE-2022-41103	Microsoft Word Information Disclosure Vulnerability	5.5	More Details
CVE-2022-41104	Microsoft Excel Security Feature Bypass Vulnerability	5.5	More Details
CVE-2022-34331	After performing a sequence of Power FW950, FW1010 maintenance operations a SRIOV network adapter can be improperly configured leading to desired VEPA configuration being disabled. IBM X-Force ID: 229695.	5.5	More Details
CVE-2022-37290	GNOME Nautilus 42.2 allows a NULL pointer dereference and get_basename application crash via a pasted ZIP archive.	5.5	More Details
CVE-2022-41098	Windows GDI+ Information Disclosure Vulnerability	5.5	More Details
CVE-2022-42786	Multiple W&T Products of the ComServer Series are prone to an XSS attack. An authenticated remote Attacker can execute arbitrary web scripts or HTML via a crafted payload injected into the title of the configuration webpage	5.4	More Details
CVE-2022-43687	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 does not issue a new session ID upon successful OAuth authentication. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42111	A Cross-site scripting (XSS) vulnerability in the Sharing module's user notification in Liferay Portal 7.2.1 through 7.4.2, and Liferay DXP 7.2 before fix pack 19, and 7.3 before update 4 allows remote attackers to inject arbitrary web script or HTML by sharing an asset with a crafted payload.	5.4	More Details
CVE-2022-44590	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in James Lao's Simple Video Embedder plugin <= 2.2 on WordPress.	5.4	More Details
CVE-2022-41091	Windows Mark of the Web Security Feature Bypass Vulnerability	5.4	More Details
CVE-2022-42119	Certain Liferay products are vulnerable to Cross Site Scripting (XSS) via the Commerce module. This affects Liferay Portal 7.3.5 through 7.4.2 and Liferay DXP 7.3 before update 8.	5.4	More Details
CVE-2022-26088	An issue was discovered in BMC Remedy before 22.1. Email-based Incident Forwarding allows remote authenticated users to inject HTML (such as an SSRF payload) into the Activity Log by placing it in the To: field. This affects rendering that occurs upon a click in the "number of recipients" field. NOTE: the vendor's position is that "no real impact is demonstrated."	5.4	More Details
CVE-2022-41049	Windows Mark of the Web Security Feature Bypass Vulnerability	5.4	More Details
CVE-2022-40844	In Tenda (Shenzhen Tenda Technology Co., Ltd) AC1200 Router model W15Ev2 V15.11.0.10(1576), a Stored Cross Site Scripting (XSS) issue exists allowing an attacker to execute JavaScript code via the applications website filtering tab, specifically the URL body.	5.4	More Details
CVE-2022-27639	Incomplete cleanup in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via adjacent access.	5.4	More Details
CVE-2022-44390	A cross-site scripting (XSS) vulnerability in EyouCMS V1.5.9-UTF8-SP1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Public Security Record Number text field.	5.4	More Details
CVE-2022-43342	A stored cross-site scripting (XSS) vulnerability in the Add function of Eramba GRC Software c2.8.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the KPI Title text field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45380	Jenkins JUnit Plugin 1159.v0b_396e1e07dd and earlier converts HTTP(S) URLs in test report output to clickable links in an unsafe manner, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-40753	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 236688.	5.4	More Details
CVE-2022-34315	IBM CICS TX 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 229451.	5.4	More Details
CVE-2022-34317	IBM CICS TX 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 229459.	5.4	More Details
CVE-2022-45401	Jenkins Associated Files Plugin 0.2.1 and earlier does not escape names of associated files, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-43488	Cross-Site Request Forgery (CSRF) vulnerability in Advanced Dynamic Pricing for WooCommerce plugin <= 4.1.5 on WordPress leading to rule type migration.	5.4	More Details
CVE-2022-36776	IBM Cloud Pak for Security (CP4S) 1.10.0.0 79and 1.10.2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 233663.	5.4	More Details
CVE-2022-40750	IBM WebSphere Application Server 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 236588.	5.4	More Details
CVE-2022-30768	A Stored Cross Site Scripting (XSS) issue in ZoneMinder 1.36.12 allows an attacker to execute HTML or JavaScript code via the Username field when an Admin (or non-Admin users that can see other users logged into the platform) clicks on Logout. NOTE: this exists in later versions than CVE-2019-7348 and requires a different attack method.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45387	Jenkins BART Plugin 1.0.3 and earlier does not escape the parsed content of build logs before rendering it on the Jenkins UI, resulting in a stored cross-site scripting (XSS) vulnerability.	5.4	More Details
CVE-2022-45382	Jenkins Naginator Plugin 1.18.1 and earlier does not escape display names of source builds in builds that were triggered via Retry action, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to edit build display names.	5.4	More Details
CVE-2022-36022	Deeplearning4J is a suite of tools for deploying and training deep learning models using the JVM. Packages org.deeplearning4j:dl4j-examples and org.deeplearning4j:platform-tests through version 1.0.0-M2.1 may use some unclaimed S3 buckets in tests in examples. This is likely affect people who use some older NLP examples that reference an old S3 bucket. The problem has been patched. Users should upgrade to snapshots as Deeplearning4J plan to publish a release with the fix at a later date. As a workaround, download a word2vec google news vector from a new source using git lfs from here.	5.3	More Details
CVE-2022-3967	A vulnerability, which was classified as critical, was found in Vesta Control Panel. Affected is an unknown function of the file func/main.sh of the component sed Handler. The manipulation leads to argument injection. An attack has to be approached locally. The name of the patch is 39561c32c12cabe563de48cc96eccb9e2c655e25. It is recommended to apply a patch to fix this issue. VDB-213546 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2022-42128	The Hypermedia REST APIs module in Liferay Portal 7.4.1 through 7.4.3.4, and Liferay DXP 7.4 GA does not properly check permissions, which allows remote attackers to obtain a WikiNode object via the WikiNodeResource.getSiteWikiNodeByExternalReferenceCode API.	5.3	More Details
CVE-2022-42127	The Friendly Url module in Liferay Portal 7.4.3.5 through 7.4.3.36, and Liferay DXP 7.4 update 1 though 36 does not properly check user permissions, which allows remote attackers to obtain the history of all friendly URLs that was assigned to a page.	5.3	More Details
CVE-2022-31772	IBM MQ 8.0, 9.0 LTS, 9.1 CD, 9.1 LTS, 9.2 CD, and 9.2 LTS could allow an authenticated and authorized user to cause a denial of service to the MQTT channels. IBM X-Force ID: 228335.	5.3	More Details
CVE-2021-38828	Xiongmai Camera XM-JPR2-LX V4.02.R12.A6420987.10002.147502.00000 is vulnerable to plain-text traffic sniffing.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3818	An uncontrolled resource consumption issue when parsing URLs in GitLab CE/EE affecting all versions prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to cause performance issues and potentially a denial of service on the GitLab instance.	5.3	More Details
CVE-2022-3285	Bypass of healthcheck endpoint allow list affecting all versions from 12.0 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows an unauthorized attacker to prevent access to GitLab	5.3	More Details
CVE-2022-3945	Improper Restriction of Excessive Authentication Attempts in GitHub repository kareadita/kavita prior to 0.6.0.3.	5.3	More Details
CVE-2022-20941	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to access sensitive information. This vulnerability is due to missing authorization for certain resources in the web-based management interface together with insufficient entropy in these resource names. An attacker could exploit this vulnerability by sending a series of HTTPS requests to an affected device to enumerate resources on the device. A successful exploit could allow the attacker to retrieve sensitive information from the device.	5.3	More Details
CVE-2022-20940	A vulnerability in the TLS handler of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to gain access to sensitive information. This vulnerability is due to improper implementation of countermeasures against a Bleichenbacher attack on a device that uses SSL decryption policies. An attacker could exploit this vulnerability by sending crafted TLS messages to an affected device, which would act as an oracle and allow the attacker to carry out a chosen-ciphertext attack. A successful exploit could allow the attacker to perform cryptanalytic operations that may allow decryption of previously captured TLS sessions to the affected device.	5.3	More Details
CVE-2022-44553	The HiView module has a vulnerability of not filtering third-party apps out when the HiView module traverses to invoke the system provider. Successful exploitation of this vulnerability may cause third-party apps to start periodically.	5.3	More Details
CVE-2022-44560	The launcher module has an Intent redirection vulnerability. Successful exploitation of this vulnerability may cause launcher module data to be modified.	5.3	More Details
CVE-2022-34329	IBM CICS TX 11.7 could allow an attacker to obtain sensitive information from HTTP response headers. IBM X-Force ID: 229467.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38705	IBM CICS TX 11.1 Standard and Advanced could allow a remote attacker to bypass security restrictions, caused by a reverse tabnabbing flaw. An attacker could exploit this vulnerability and redirect a victim to a phishing site. IBM X-Force ID: 234172.	5.3	More Details
CVE-2022-39881	Improper input validation vulnerability for processing SIB12 PDU in Exynos modems prior to SMR Sep-2022 Release allows remote attacker to read out of bounds memory.	5.3	More Details
CVE-2021-26251	Improper input validation in the Intel(R) Distribution of OpenVINO(TM) Toolkit may allow an authenticated user to potentially enable denial of service via network access.	5.3	More Details
CVE-2022-3941	A vulnerability has been found in Activity Log Plugin and classified as critical. This vulnerability affects unknown code of the component HTTP Header Handler. The manipulation of the argument X-Forwarded-For leads to improper output neutralization for logs. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-213448.	5.3	More Details
CVE-2022-45389	A missing permission check in Jenkins XP-Dev Plugin 1.0 and earlier allows unauthenticated attackers to trigger builds of jobs corresponding to an attacker-specified repository.	5.3	More Details
CVE-2022-43691	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 inadvertently disclose server-side sensitive information (secrets in environment variables and server information) when Debug Mode is left on in production.	5.3	More Details
CVE-2022-43689	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to XXE based DNS requests leading to IP disclosure.	5.3	More Details
CVE-2022-45195	SimpleXMQ before 3.4.0, as used in SimpleX Chat before 4.2, does not apply a key derivation function to intended data, which can interfere with forward secrecy and can have other impacts if there is a compromise of a single private key. This occurs in the X3DH key exchange for the double ratchet protocol.	5.3	More Details
CVE-2022-36349	Insecure default variable initialization in BIOS firmware for some Intel(R) NUC Boards and Intel(R) NUC Kits before version MYi30060 may allow an authenticated user to potentially enable denial of service via local access.	5.2	More Details
CVE-2022-35719	IBM MQ Internet Pass-Thru 2.1, 9.2 LTS and 9.2 CD stores potentially sensitive information in trace files that could be read by a local user.	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3866	HashiCorp Nomad and Nomad Enterprise 1.4.0 up to 1.4.1 workload identity token can list non-sensitive metadata for paths under nomad/ that belong to other jobs in the same namespace. Fixed in 1.4.2.	5.0	More Details
CVE-2022-40843	The Tenda AC1200 V-W15Ev2 V15.11.0.10(1576) router is vulnerable to improper authorization / improper session management that allows the router login page to be bypassed. This leads to authenticated attackers having the ability to read the routers syslog.log file which contains the MD5 password of the Administrator's user account.	4.9	More Details
CVE-2022-20836	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2022-20872	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2022-20935	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20843	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2022-20936	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2022-20840	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2022-3631	The OAuth Client by DigitialPixies WordPress plugin through 1.1.0 does not sanitize and escapes some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in multisite setup).	4.8	More Details
CVE-2022-3539	The Testimonials WordPress plugin before 2.7, super-testimonial-pro WordPress plugin before 1.0.8 do not sanitize and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3469	The WP Attachments WordPress plugin before 5.0.5 does not sanitize and escapes some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in multisite setup).	4.8	More Details
CVE-2022-20839	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2022-20838	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2022-42131	Certain Liferay products are affected by: Missing SSL Certificate Validation in the Dynamic Data Mapping module's REST data providers. This affects Liferay Portal 7.1.0 through 7.4.2 and Liferay DXP 7.1 before fix pack 27, 7.2 before fix pack 17, and 7.3 before service pack 3.	4.8	More Details
CVE-2022-20905	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43695	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Stored Cross-Site Scripting (XSS) in dashboard/system/express/entities/associations because Concrete CMS allows association with an entity name that doesn't exist or, if it does exist, contains XSS since it was not properly sanitized. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+.	4.8	More Details
CVE-2022-20835	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2022-43688	Concrete CMS (formerly concrete5) below 8.5.10 and between 9.0.0 and 9.1.2 is vulnerable to Stored Cross-Site Scripting (XSS) in icons since the Microsoft application tile color is not sanitized. Remediate by updating to Concrete CMS 9.1.3+ or 8.5.10+.	4.8	More Details
CVE-2022-20834	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2022-3726	Lack of sand-boxing of OpenAPI documents in GitLab CE/EE affecting all versions from 12.6 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to trick a user to click on the Swagger OpenAPI viewer and issue HTTP requests that affect the victim's account.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20833	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2022-20832	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2022-20831	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2022-40846	In Tenda AC1200 Router model W15Ev2 V15.11.0.10(1576), a Stored Cross Site Scripting (XSS) vulnerability exists allowing an attacker to execute JavaScript code via the applications stored hostname.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20932	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2022-3486	An open redirect vulnerability in GitLab EE/CE affecting all versions from 9.3 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2, allows an attacker to redirect users to an arbitrary location if they trust the URL.	4.7	More Details
CVE-2022-3903	An incorrect read request flaw was found in the Infrared Transceiver USB driver in the Linux kernel. This issue occurs when a user attaches a malicious USB device. A local user could use this flaw to starve the resources, causing denial of service or potentially crashing the system.	4.6	More Details
CVE-2022-3971	A vulnerability was found in matrix-appservice-irc up to 0.35.1. It has been declared as critical. This vulnerability affects unknown code of the file src/datastore/postgres/PgDataStore.ts. The manipulation of the argument roomIds leads to sql injection. Upgrading to version 0.36.0 is able to address this issue. The name of the patch is 179313a37f06b298150edba3e2b0e5a73c1415e7. It is recommended to upgrade the affected component. VDB-213550 is the identifier assigned to this vulnerability.	4.6	More Details
CVE-2022-41099	BitLocker Security Feature Bypass Vulnerability	4.6	More Details
CVE-2022-30769	Session fixation exists in ZoneMinder through 1.36.12 as an attacker can poison a session cookie to the next logged-in user.	4.6	More Details
CVE-2022-36367	Incorrect default permissions in the Intel(R) Support Android application before version v22.02.28 may allow a privileged user to potentially enable information disclosure via local access.	4.4	More Details
CVE-2022-41066	Microsoft Business Central Information Disclosure Vulnerability	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29486	Improper buffer restrictions in the Hyperscan library maintained by Intel(R) all versions downloaded before 04/29/2022 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	4.3	More Details
CVE-2022-3964	A vulnerability classified as problematic has been found in ffmpeg. This affects an unknown part of the file libavcodec/rpzaenc.c of the component QuickTime RPZA Video Encoder. The manipulation of the argument y_size leads to out-of-bounds read. It is possible to initiate the attack remotely. The name of the patch is 92f9b28ed84a77138105475beba16c146bdaf984. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-213543.	4.3	More Details
CVE-2022-45390	A missing permission check in Jenkins loader.io Plugin 1.0.1 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2022-45394	A missing permission check in Jenkins Delete log Plugin 1.0 and earlier allows attackers with Item/Read permission to delete build logs.	4.3	More Details
CVE-2022-42130	The Dynamic Data Mapping module in Liferay Portal 7.1.0 through 7.4.3.4, and Liferay DXP 7.1 before fix pack 27, 7.2 before fix pack 19, 7.3 before update 4, and 7.4 GA does not properly check permission of form entries, which allows remote authenticated users to view and access all form entries.	4.3	More Details
CVE-2022-45399	A missing permission check in Jenkins Cluster Statistics Plugin 0.4.6 and earlier allows attackers to delete recorded Jenkins Cluster Statistics.	4.3	More Details
CVE-2022-39884	Improper access control vulnerability in IImsService prior to SMR Nov-2022 Release 1 allows local attacker to access to Call information.	4.3	More Details
CVE-2022-26047	Improper input validation for some Intel(R) PROSet/Wireless WiFi, Intel vPro(R) CSME WiFi and Killer(TM) WiFi products may allow unauthenticated user to potentially enable denial of service via local access.	4.3	More Details
CVE-2022-34313	IBM CICS TX 11.1 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. X-Force ID: 229449.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3965	A vulnerability classified as problematic was found in ffmpeg. This vulnerability affects the function smc_encode_stream of the file libavcodec/smcenc.c of the component QuickTime Graphics Video Encoder. The manipulation of the argument y_size leads to out-of-bounds read. The attack can be initiated remotely. The name of the patch is 13c13109759090b7f7182480d075e13b36ed8edd. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-213544.	4.3	More Details
CVE-2022-20938	A vulnerability in the module import function of the administrative interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to view sensitive information. This vulnerability is due to insufficient validation of the XML syntax when importing a module. An attacker could exploit this vulnerability by supplying a specially crafted XML file to the function. A successful exploit could allow the attacker to read sensitive data that would normally not be revealed.	4.3	More Details
CVE-2022-3966	A vulnerability, which was classified as critical, has been found in Ultimate Member Plugin up to 2.5.0. This issue affects the function load_template of the file includes/core/class-shortcodes.php of the component Template Handler. The manipulation of the argument tpl leads to pathname traversal. The attack may be initiated remotely. Upgrading to version 2.5.1 is able to address this issue. The name of the patch is e1bc94c1100f02a129721ba4be5fbc44c3d78ec4. It is recommended to upgrade the affected component. The identifier VDB-213545 was assigned to this vulnerability.	4.3	More Details
CVE-2022-26508	Improper authentication in the Intel(R) SDP Tool before version 3.0.0 may allow an unauthenticated user to potentially enable information disclosure via network access.	4.3	More Details
CVE-2022-3978	A vulnerability, which was classified as problematic, was found in NodeBB up to 2.5.7. This affects an unknown part of the file /register/abort. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. Upgrading to version 2.5.8 is able to address this issue. The name of the patch is 2f9d8c350e54543f608d3d4c8e1a49bbb6cdea38. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-213555.	4.3	More Details
CVE-2022-3957	A vulnerability classified as problematic was found in GPAC. Affected by this vulnerability is the function svg_parse_preserveaspectratio of the file scenegraph/svg_attributes.c of the component SVG Parser. The manipulation leads to memory leak. The attack can be launched remotely. The name of the patch is 2191e66aa7df750e8ef01781b1930bea87b713bb. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-213463.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3447	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 106.0.5249.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2022-39887	Improper access control vulnerability in clearAllGlobalProxy in MiscPolicy prior to SMR Nov-2022 Release 1 allows local attacker to configure EDM setting.	4.3	More Details
CVE-2022-2450	The reSmush.it : the only free Image Optimizer & compress plugin WordPress plugin before 0.4.4 lacks authorization in various AJAX actions, allowing any logged-in users, such as subscribers to call them.	4.3	More Details
CVE-2022-44548	There is a vulnerability in permission verification during the Bluetooth pairing process. Successful exploitation of this vulnerability may cause the dialog box for confirming the pairing not to be displayed during Bluetooth pairing.	4.3	More Details
CVE-2022-45398	A cross-site request forgery (CSRF) vulnerability in Jenkins Cluster Statistics Plugin 0.4.6 and earlier allows attackers to delete recorded Jenkins Cluster Statistics.	4.3	More Details
CVE-2022-41913	Discourse-calendar is a plugin for the Discourse messaging platform which adds the ability to create a dynamic calendar in the first post of a topic. Members of private groups or public groups with private members can be listed by users, who can create and edit post events. This vulnerability only affects sites which have discourse post events enabled. This issue has been patched in commit `ca5ae3e7e` which will be included in future releases. Users unable to upgrade should disable the `discourse_post_event_enabled` setting to fully mitigate the issue. Also, it's possible to prevent regular users from using this vulnerability by removing all groups from the `discourse_post_event_allowed_on_groups` but note that moderators will still be able to use it.	4.3	More Details
CVE-2022-42129	An Insecure direct object reference (IDOR) vulnerability in the Dynamic Data Mapping module in Liferay Portal 7.3.2 through 7.4.3.4, and Liferay DXP 7.3 before update 4, and 7.4 GA allows remote authenticated users to view and access form entries via the `formInstanceRecordId` parameter.	4.3	More Details
CVE-2022-3793	An improper authorization issue in GitLab CE/EE affecting all versions from 14.4 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to read variables set directly in a GitLab CI/CD configuration file they don't have access to.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3413	Incorrect authorization during display of Audit Events in GitLab EE affecting all versions from 14.5 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2, allowed Developers to view the project's Audit Events and Developers or Maintainers to view the group's Audit Events. These should have been restricted to Project Maintainers, Group Owners, and above.	4.3	More Details
CVE-2022-31255	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in spacewalk/Uyuni of SUSE Linux Enterprise Module for SUSE Manager Server 4.2, SUSE Linux Enterprise Module for SUSE Manager Server 4.3, SUSE Manager Server 4.2 allows remote attackers to read files available to the user running the process, typically tomcat. This issue affects: SUSE Linux Enterprise Module for SUSE Manager Server 4.2 hub-xmlrpc-api-0.7-150300.3.9.2, inter-server-sync-0.2.4-150300.8.25.2, locale-formula-0.3-150300.3.3.2, py27-compat-salt-3000.3-150300.7.7.26.2, python-urlgrabber-3.10.2.1py2_3-150300.3.3.2, spacecmd-4.2.20-150300.4.30.2, spacewalk-backend-4.2.25-150300.4.32.4, spacewalk-client-tools-4.2.21-150300.4.27.3, spacewalk-java-4.2.43-150300.3.48.2, spacewalk-utils-4.2.18-150300.3.21.2, spacewalk-web-4.2.30-150300.3.30.3, susemanager-4.2.38-150300.3.44.3, susemanager-doc-indexes-4.2-150300.12.36.3, susemanager-docs_en-4.2-150300.12.36.2, susemanager-schema-4.2.25-150300.3.30.3, susemanager-sls versions prior to 4.2.28. SUSE Linux Enterprise Module for SUSE Manager Server 4.3 spacewalk-java versions prior to 4.3.39. SUSE Manager Server 4.2 release-notes-susemanager versions prior to 4.2.10.	4.3	More Details
CVE-2022-2761	An information disclosure issue in GitLab CE/EE affecting all versions from 14.4 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to use GitLab Flavored Markdown (GFM) references in a Jira issue to disclose the names of resources they don't have access to.	4.3	More Details
CVE-2022-39891	Heap overflow vulnerability in parse_pce function in libsavsaudio.so in Editor Lite prior to version 4.0.41.3 allows attacker to get information.	4.3	More Details
CVE-2022-42126	The Asset Libraries module in Liferay Portal 7.3.5 through 7.4.3.28, and Liferay DXP 7.3 before update 8, and DXP 7.4 before update 29 does not properly check permissions of asset libraries, which allows remote authenticated users to view asset libraries via the UI.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43753	A Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in spacewalk/Uyuni of SUSE Linux Enterprise Module for SUSE Manager Server 4.2, SUSE Linux Enterprise Module for SUSE Manager Server 4.3, SUSE Manager Server 4.2 allows remote attackers to read files available to the user running the process, typically tomcat. This issue affects: SUSE Linux Enterprise Module for SUSE Manager Server 4.2 hub-xmlrpc-api-0.7-150300.3.9.2, inter-server-sync-0.2.4-150300.8.25.2, locale-formula-0.3-150300.3.3.2, py27-compat-salt-3000.3-150300.7.7.26.2, python-urlgrabber-3.10.2.1py2_3-150300.3.3.2, spacecmd-4.2.20-150300.4.30.2, spacewalk-backend-4.2.25-150300.4.32.4, spacewalk-client-tools-4.2.21-150300.4.27.3, spacewalk-java-4.2.43-150300.3.48.2, spacewalk-utils-4.2.18-150300.3.21.2, spacewalk-web-4.2.30-150300.3.30.3, susemanager-4.2.38-150300.3.44.3, susemanager-doc-indexes-4.2-150300.12.36.3, susemanager-docs_en-4.2-150300.12.36.2, susemanager-schema-4.2.25-150300.3.30.3, susemanager-sls versions prior to 4.2.28. SUSE Linux Enterprise Module for SUSE Manager Server 4.3 spacewalk-java versions prior to 4.3.39. SUSE Manager Server 4.2 release-notes-susemanager versions prior to 4.2.10.	4.3	More Details
CVE-2022-40309	Users with write permissions to a repository can delete arbitrary directories.	4.3	More Details
CVE-2022-3942	A vulnerability was found in SourceCodester Sanitization Management System and classified as problematic. This issue affects some unknown processing of the file php-sms/?p=request_quote. The manipulation leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-213449 was assigned to this vulnerability.	4.3	More Details
CVE-2022-27895	Information Exposure Through Log Files vulnerability discovered in Foundry when logs were captured using an underlying library known as Build2. This issue was present in versions earlier than 1.785.0. Upgrade to Build2 version 1.785.0 or greater.	4.2	More Details
CVE-2022-43679	The Docker image of ownCloud Server through 10.11 contains a misconfiguration that renders the trusted_domains config useless. This could be abused to spoof the URL in password-reset e-mail messages.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41873	Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. Versions prior to 4.9 are vulnerable to an Out-of-bounds read. While processing the L2CAP protocol, the Bluetooth Low Energy stack of Contiki-NG needs to map an incoming channel ID to its metadata structure. While looking up the corresponding channel structure in get_channel_for_cid (in os/net/mac/ble/ble-l2cap.c), a bounds check is performed on the incoming channel ID, which is meant to ensure that the channel ID does not exceed the maximum number of supported channels.However, an integer truncation issue leads to only the lowest byte of the channel ID to be checked, which leads to an incomplete out-of-bounds check. A crafted channel ID leads to out-of-bounds memory to be read and written with attacker-controlled data. The vulnerability has been patched in the "develop" branch of Contiki-NG, and will be included in release 4.9. As a workaround, Users can apply the patch in Contiki-NG pull request 2081 on GitHub.	4.2	More Details
CVE-2022-27896	Information Exposure Through Log Files vulnerability discovered in Foundry Code-Workbooks where the endpoint backing that console was generating service log records of any Python code being run. These service logs included the Foundry token that represents the Code-Workbooks Python console. Upgrade to Code-Workbooks version 4.461.0. This issue affects Palantir Foundry Code-Workbooks version 4.144 to version 4.460.0 and is resolved in 4.461.0.	4.2	More Details
CVE-2022-34312	IBM CICS TX 11.1 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 229447.	4.0	More Details
CVE-2022-39883	Improper authorization vulnerability in StorageManagerService prior to SMR Nov-2022 Release 1 allows local attacker to call privileged API.	4.0	More Details
CVE-2022-3895	Some UI elements of the Common User Interface Component are not properly sanitizing output and therefore prone to output arbitrary HTML (XSS).	4.0	More Details
CVE-2022-34314	IBM CICS TX 11.1 could disclose sensitive information to a local user due to insecure permission settings. IBM X-Force ID: 229450.	4.0	More Details
CVE-2022-39889	Improper access control vulnerability in GalaxyWatch4Plugin prior to versions 2.2.11.22101351 and 2.2.12.22101351 allows attackers to access wearable device information.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39394	Wasmtime is a standalone runtime for WebAssembly. Prior to version 2.0.2, there is a bug in Wasmtime's C API implementation where the definition of the `wasmtime_trap_code` does not match its declared signature in the `wasmtime/trap.h` header file. This discrepancy causes the function implementation to perform a 4-byte write into a 1-byte buffer provided by the caller. This can lead to three zero bytes being written beyond the 1-byte location provided by the caller. This bug has been patched and users should upgrade to Wasmtime 2.0.2. This bug can be worked around by providing a 4-byte buffer casted to a 1-byte buffer when calling `wasmtime_trap_code`. Users of the `wasmtime` crate are not affected by this issue, only users of the C API function `wasmtime_trap_code` are affected.	3.8	More Details
CVE-2022-45194	CBRN-Analysis before 22 allows XXE attacks via am mws XML document, leading to NTLMv2-SSP hash disclosure.	3.8	More Details
CVE-2022-30297	Cross-site scripting in the Intel(R) EMA software before version 1.8.0 may allow a privileged user to potentially enable escalation of privilege via local access.	3.8	More Details
CVE-2022-4006	A vulnerability, which was classified as problematic, has been found in WBCE CMS. Affected by this issue is the function increase_attempts of the file wbce/framework/class.login.php of the component Header Handler. The manipulation of the argument X-Forwarded-For leads to improper restriction of excessive authentication attempts. The attack may be launched remotely. The name of the patch is d394ba39a7bfeb31eda797b6195fd90ef74b2e75. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-213716.	3.7	More Details
CVE-2022-42965	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the snowflake-connector-python PyPI package, when an attacker is able to supply arbitrary input to the undocumented get_file_transfer_type method	3.7	More Details
CVE-2022-34316	IBM CICS TX 11.1 does not neutralize or incorrectly neutralizes web scripting syntax in HTTP headers that can be used by web browser components that can process raw headers. IBM X-Force ID: 229452.	3.7	More Details
CVE-2022-39892	Improper access control in Samsung Pass prior to version 4.0.05.1 allows attackers to unauthenticated access via keep open feature.	3.6	More Details
CVE-2022-45393	A cross-site request forgery (CSRF) vulnerability in Jenkins Delete log Plugin 1.0 and earlier allows attackers to delete build logs.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3950	A vulnerability, which was classified as problematic, was found in sanluan PublicCMS. Affected is the function initLink of the file dwz.min.js of the component Tab Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is a972dc9b1c94aea2d84478bf26283904c21e4ca2. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-213456.	3.5	More Details
CVE-2022-3280	An open redirect in GitLab CE/EE affecting all versions from 10.1 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows an attacker to trick users into visiting a trustworthy URL and being redirected to arbitrary content.	3.5	More Details
CVE-2022-3943	A vulnerability was found in ForU CMS. It has been classified as problematic. Affected is an unknown function of the file cms_chip.php. The manipulation of the argument name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-213450 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-3975	A vulnerability, which was classified as problematic, has been found in NukeViet CMS. Affected by this issue is the function filterAttr of the file vendor/vinades/nukeviet/Core/Request.php of the component Data URL Handler. The manipulation of the argument attrSubSet leads to cross site scripting. The attack may be launched remotely. Upgrading to version 4.5 is able to address this issue. The name of the patch is 0b3197fad950bb3383e83039a8ee4c9509b3ce02. It is recommended to upgrade the affected component. VDB-213554 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-3940	A vulnerability, which was classified as problematic, was found in lanyulei ferry. This affects an unknown part of the file apis/process/task.go. The manipulation of the argument file_name leads to path traversal. The associated identifier of this vulnerability is VDB-213447.	3.5	More Details
CVE-2022-3968	A vulnerability has been found in emlog and classified as problematic. Affected by this vulnerability is an unknown functionality of the file admin/article_save.php. The manipulation of the argument tag leads to cross site scripting. The attack can be launched remotely. The name of the patch is 5bf7a79826e0ea09bcc8a21f69a0c74107761a02. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-213547.	3.5	More Details
CVE-2022-3819	An improper authorization issue in GitLab CE/EE affecting all versions from 15.0 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows a malicious users to set emojis on internal notes they don't have access to.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3963	A vulnerability was found in gnuboard5. It has been classified as problematic. Affected is an unknown function of the file bbs/faq.php of the component FAQ Key ID Handler. The manipulation of the argument fm_id leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 5.5.8.2.1 is able to address this issue. The name of the patch is ba062ca5b62809106d5a2f7df942ffcb44ecb5a9. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-213540.	3.5	More Details
CVE-2022-3949	A vulnerability, which was classified as problematic, has been found in Sourcecodester Simple Cashiering System. This issue affects some unknown processing of the component User Account Handler. The manipulation of the argument fullname leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-213455.	3.5	More Details
CVE-2022-3988	A vulnerability was found in Frappe. It has been rated as problematic. Affected by this issue is some unknown functionality of the file frappe/templates/includes/navbar/navbar_search.html of the component Search. The manipulation of the argument q leads to cross site scripting. The attack may be launched remotely. The name of the patch is bfab7191543961c6cb77fe267063877c31b616ce. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-213560.	3.5	More Details
CVE-2022-28764	The Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows) before version 5.12.6 is susceptible to a local information exposure vulnerability. A failure to clear data from a local SQL database after a meeting ends and the usage of an insufficiently secure per-device key encrypting that database results in a local malicious user being able to obtain meeting information such as in-meeting chat for the previous meeting attended from that local user account.	3.3	More Details
CVE-2022-33973	Improper access control in the Intel(R) WAPI Security software for Windows 10/11 before version 22.2150.0.1 may allow an authenticated user to potentially enable information disclosure via local access.	3.3	More Details
CVE-2022-26045	Improper buffer restrictions in some Intel(R) XMM(TM) 7560 Modem software before version M2_7560_R_01.2146.00 may allow a privileged user to potentially enable escalation of privilege via physical access.	3.3	More Details
CVE-2022-39893	Sensitive information exposure vulnerability in FmmBaseModel in Galaxy Buds Pro Manage prior to version 4.1.22092751 allows local attackers with log access permission to get device identifier data through device log.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42001	Cross-site Scripting (XSS) vulnerability in BlueSpiceBookshelf extension of BlueSpice allows user with regular account and edit permissions to inject arbitrary HTML into the book navigation.	3.3	More Details
CVE-2022-42000	Cross-site Scripting (XSS) vulnerability in BlueSpiceSocialProfile extension of BlueSpice allows user with comment permissions to inject arbitrary HTML into the comment section of a wikipage.	3.3	More Details
CVE-2022-41814	Cross-site Scripting (XSS) vulnerability in BlueSpiceFoundation extension of BlueSpice allows user with regular account and edit permissions to inject arbitrary HTML into the history view of a wikipage.	3.3	More Details
CVE-2022-41789	Cross-site Scripting (XSS) vulnerability in BlueSpiceDiscovery skin of BlueSpice allows logged in user with edit permissions to inject arbitrary HTML into the default page header of a wikipage.	3.3	More Details
CVE-2022-3958	Cross-site Scripting (XSS) vulnerability in BlueSpiceUserSidebar extension of BlueSpice allows user with regular account and edit permissions to inject arbitrary HTML into the personal menu navigation of their own and other users. This allows for targeted attacks.	3.3	More Details
CVE-2022-3706	Improper authorization in GitLab CE/EE affecting all versions from 7.14 prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows a user retrying a job in a downstream pipeline to take ownership of the retried jobs in the upstream pipeline even if the user doesn't have access to that project.	3.1	More Details
CVE-2022-3959	A vulnerability, which was classified as problematic, has been found in drogon up to 1.8.1. Affected by this issue is some unknown functionality of the component Session Hash Handler. The manipulation leads to small space of random values. The attack may be launched remotely. Upgrading to version 1.8.2 is able to address this issue. The name of the patch is c0d48da99f66aaada17bcd28b07741cac8697647. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-213464.	3.1	More Details
CVE-2022-3867	HashiCorp Nomad and Nomad Enterprise 1.4.0 up to 1.4.1 event stream subscribers using a token with TTL receive updates until token garbage is collected. Fixed in 1.4.2.	2.7	More Details
CVE-2022-3969	A vulnerability was found in OpenKM up to 6.3.11 and classified as problematic. Affected by this issue is the function getFileExtension of the file src/main/java/com/openkm/util/FileUtils.java. The manipulation leads to insecure temporary file. Upgrading to version 6.3.12 is able to address this issue. The name of the patch is c069e4d73ab8864345c25119d8459495f45453e1. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-213548.	2.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4241	A vulnerability, which was classified as problematic, was found in phpservermon. Affected is the function setUserLoggedIn of the file src/psm/Service/User.php. The manipulation leads to use of predictable algorithm in random number generator. The exploit has been disclosed to the public and may be used. The name of the patch is bb10a5f3c68527c58073258cb12446782d223bc3. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-213744.	2.6	More Details
CVE-2021-4240	A vulnerability, which was classified as problematic, was found in phpservermon. This affects the function generatePasswordResetToken of the file src/psm/Service/User.php. The manipulation leads to use of predictable algorithm in random number generator. The exploit has been disclosed to the public and may be used. The name of the patch is 3daa804d5f56c55b3ae13bfac368bb84ec632193. It is recommended to apply a patch to fix this issue. The identifier VDB-213717 was assigned to this vulnerability.	2.6	More Details
CVE-2022-3952	A vulnerability has been found in ManyDesigns Portofino 5.3.2 and classified as problematic. Affected by this vulnerability is the function createTempDir of the file WarFileLauncher.java. The manipulation leads to creation of temporary file in directory with insecure permissions. Upgrading to version 5.3.3 is able to address this issue. The name of the patch is 94653cb357806c9cf24d8d294e6afea33f8f0775. It is recommended to upgrade the affected component. The identifier VDB-213457 was assigned to this vulnerability.	2.6	More Details
CVE-2022-41874	Tauri is a framework for building binaries for all major desktop platforms. In versions prior to 1.0.7 and 1.1.2, Tauri is vulnerable to an Incorrectly-Resolved Name. Due to incorrect escaping of special characters in paths selected via the file dialog and drag and drop functionality, it is possible to partially bypass the `fs` scope definition. It is not possible to traverse into arbitrary paths, as the issue is limited to neighboring files and sub folders of already allowed paths. The impact differs on Windows, MacOS and Linux due to different specifications of valid path characters. This bypass depends on the file picker dialog or dragged files, as user selected paths are automatically added to the allow list at runtime. A successful bypass requires the user to select a pre-existing malicious file or directory during the file picker dialog and an adversary controlled logic to access these files. The issue has been patched in versions 1.0.7, 1.1.2 and 1.2.0. As a workaround, disable the dialog and fileDropEnabled component inside the tauri.conf.json.	2.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43754	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in spacewalk/Uyuni of SUSE Linux Enterprise Module for SUSE Manager Server 4.2, SUSE Linux Enterprise Module for SUSE Manager Server 4.3, SUSE Manager Server 4.2 allows remote attackers to embed Javascript code via /rhn/audit/scap/Search.do This issue affects: SUSE Linux Enterprise Module for SUSE Manager Server 4.2 hub-xmlrpc-api-0.7-150300.3.9.2, inter-server-sync-0.2.4-150300.8.25.2, locale-formula-0.3-150300.3.3.2, py27-compat-salt-3000.3-150300.7.7.26.2, python-urlgrabber-3.10.2.1py2_3-150300.3.3.2, spacecmd-4.2.20-150300.4.30.2, spacewalk-backend-4.2.25-150300.4.32.4, spacewalk-client-tools-4.2.21-150300.4.27.3, spacewalk-java-4.2.43-150300.3.48.2, spacewalk-utils-4.2.18-150300.3.21.2, spacewalk-web-4.2.30-150300.3.30.3, susemanager-4.2.38-150300.3.44.3, susemanager-doc-indexes-4.2-150300.12.36.3, susemanager-docs_en-4.2-150300.12.36.2, susemanager-schema-4.2.25-150300.3.30.3, susemanager-sls versions prior to 4.2.28. SUSE Linux Enterprise Module for SUSE Manager Server 4.3 spacewalk-java versions prior to 4.3.39. SUSE Manager Server 4.2 release-notes-susemanager versions prior to 4.2.10.	2.6	More Details
CVE-2022-27499	Premature release of resource during expected lifetime in the Intel(R) SGX SDK software may allow a privileged user to potentially enable information disclosure via local access.	2.5	More Details
CVE-2022-3992	A vulnerability classified as problematic was found in SourceCodester Sanitization Management System. Affected by this vulnerability is an unknown functionality of the file admin/?page=system_info of the component Banner Image Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-213571.	2.4	More Details
CVE-2022-3893	Cross-site Scripting (XSS) vulnerability in BlueSpiceCustomMenu extension of BlueSpice allows user with admin permissions to inject arbitrary HTML into the custom menu navigation of the application.	2.3	More Details
CVE-2022-41611	Cross-site Scripting (XSS) vulnerability in BlueSpiceDiscovery skin of BlueSpice allows user with admin privileges to inject arbitrary HTML into the main navigation of the application.	2.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29836	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability was discovered via an HTTP API on Western Digital My Cloud Home; My Cloud Home Duo; and SanDisk ibi devices that could allow an attacker to abuse certain parameters to point to random locations on the file system. This could also allow the attacker to initiate the installation of custom packages at these locations. This can only be exploited once the attacker has been authenticated to the device. This issue affects: Western Digital My Cloud Home and My Cloud Home Duo versions prior to 8.11.0-113 on Linux; SanDisk ibi versions prior to 8.11.0-113 on Linux.	1.9	More Details
CVE-2022-3953	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-28748	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-2964. Reason: This candidate is a reservation duplicate of CVE-2022-2964. Notes: All CVE users should reference CVE-2022-2964 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2022-39390	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-36534. Reason: This candidate is a reservation duplicate of CVE-2020-36534. Notes: All CVE users should reference CVE-2020-36534 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details