SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 17 May 2023

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-2023-31471	An issue was discovered on GL.iNet devices before 3.216. Through the software installation feature, it is possible to install arbitrary software, such as a reverse shell, because the restrictions on the available package list are limited to client-side verification. It is possible to install software from the filesystem, the package list, or a URL.	9.8	More Details
CVE-2023-30352	Shenzen Tenda Technology IP Camera CP3 V11.10.00.2211041355 was discovered to contain a hard-coded default password for the RTSP feed.	9.8	More Details
CVE-2023-31985	A Command Injection vulnerability in Edimax Wireless Router N300 Firmware BR-6428NS_v4 allows attacker to execute arbitrary code via the formAccept function in /bin/webs without any limitations.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1934	The PnPSCADA system, a product of SDG Technologies CC, is afflicted by a critical unauthenticated error-based PostgreSQL Injection vulnerability. Present within the hitlogcsv.jsp endpoint, this security flaw permits unauthenticated attackers to engage with the underlying database seamlessly and passively. Consequently, malicious actors could gain access to vital information, such as Industrial Control System (ICS) and OT data, alongside other sensitive records like SMS and SMS Logs. The unauthorized database access exposes compromised systems to potential manipulation or breach of essential infrastructure data, highlighting the severity of this vulnerability.	9.8	More Details
CVE-2023-27823	An authentication bypass in Optoma 1080PSTX C02 allows an attacker to access the administration console without valid credentials.	9.8	More Details
CVE-2023-31983	A Command Injection vulnerability in Edimax Wireless Router N300 Firmware BR-6428NS_v4 allows attacker to execute arbitrary code via the mp function in /bin/webs without any limitations.	9.8	More Details
CVE-2023-30247	File Upload vulnerability found in Oretnom23 Storage Unit Rental Management System v.1.0 allows a remote attacker to execute arbitrary code via the update_settings parameter.	9.8	More Details
CVE-2023-1096	SnapCenter versions 4.7 prior to 4.7P2 and 4.8 prior to 4.8P1 are susceptible to a vulnerability which could allow a remote unauthenticated attacker to gain access as an admin user.	9.8	More Details
CVE-2023-1698	In multiple products of WAGO a vulnerability allows an unauthenticated, remote attacker to create new users and change the device configuration which can result in unintended behaviour, Denial of Service and full system compromise.	9.8	More Details
CVE-2022-47937	Improper input validation in the Apache Sling Commons JSON bundle allows an attacker to trigger unexpected errors by supplying specially-crafted input. The org.apache.sling.commons.json bundle has been deprecated as of March 2017 and should not be used anymore. Consumers are encouraged to consider the Apache Sling Commons Johnzon OSGi bundle provided by the Apache Sling project, but may of course use other JSON libraries.	9.8	More Details
CVE-2023-31986	A Command Injection vulnerability in Edimax Wireless Router N300 Firmware BR-6428NS_v4 allows attacker to execute arbitrary code via the setWAN function in /bin/webs without any limitations.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4774	The Bit Form WordPress plugin before 1.9 does not validate the file types uploaded via it's file upload form field, allowing unauthenticated users to upload arbitrary files types such as PHP or HTML files to the server, leading to Remote Code Execution.	9.8	More Details
CVE-2023-0600	The WP Visitor Statistics (Real Time Traffic) WordPress plugin before 6.9 does not escape user input which is concatenated to an SQL query, allowing unauthenticated visitors to conduct SQL Injection attacks.	9.8	More Details
CVE-2023-29862	An issue found in Agasio-Camera device version not specified allows a remote attacker to execute arbitrary code via the check and authLevel parameters.	9.8	More Details
CVE-2023-29861	An issue found in FLIR-DVTEL version not specified allows a remote attacker to execute arbitrary code via a crafted request to the management page of the device.	9.8	More Details
CVE-2023-30245	SQL injection vulnerability found in Judging Management System v.1.0 allows a remote attacker to execute arbitrary code via the crit_id parameter of the edit_criteria.php file.	9.8	More Details
CVE-2023-32314	vm2 is a sandbox that can run untrusted code with Node's built-in modules. A sandbox escape vulnerability exists in vm2 for versions up to and including 3.9.17. It abuses an unexpected creation of a host object based on the specification of `Proxy`. As a result a threat actor can bypass the sandbox protections to gain remote code execution rights on the host running the sandbox. This vulnerability was patched in the release of version `3.9.18` of `vm2`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.8	More Details
CVE-2021-0877	Product: AndroidVersions: Android SoCAndroid ID: A-273754094	9.8	More Details
CVE-2023-29961	D-Link DIR-605L firmware version 1.17B01 BETA is vulnerable to stack overflow via /goform/formTcpipSetup,	9.8	More Details
CVE-2023-32956	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in CGI component in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows remote attackers to execute arbitrary code via unspecified vectors.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2499	The RegistrationMagic plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 5.2.1.0. This is due to insufficient verification on the user being supplied during a Google social login through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email.	9.8	More Details
CVE-2023-31519	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the email parameter at login_core.php.	9.8	More Details
CVE-2023-31587	Tenda AC5 router V15.03.06.28 was discovered to contain a remote code execution (RCE) vulnerability via the Mac parameter at ip/goform/WriteFacMac.	9.8	More Details
CVE-2023-31856	A command injection vulnerability in the hostTime parameter in the function NTPSyncWithHostof TOTOLINK CP300+ V5.2cu.7594_B20200910 allows attackers to execute arbitrary commands via a crafted http packet.	9.8	More Details
CVE-2023-31857	Sourcecodester Online Computer and Laptop Store 1.0 allows unrestricted file upload and can lead to remote code execution. The vulnerability path is /classes/Users.php?f=save.	9.8	More Details
CVE-2023-31890	An XML Deserialization vulnerability in glazedlists v1.11.0 allows an attacker to execute arbitrary code via the BeanXMLByteCoder.decode() parameter.	9.8	More Details
CVE-2023-27742	IDURAR ERP/CRM v1 was discovered to contain a SQL injection vulnerability via the component /api/login.	9.8	More Details
CVE-2023-30246	SQL injection vulnerability found in Judging Management System v.1.0 allows a remote attacker to execute arbitrary code via the contestant_id parameter.	9.8	More Details
CVE-2023-27238	LavaLite CMS v 9.0.0 was discovered to be vulnerable to web cache poisoning.	9.8	More Details
CVE-2023-32243	Improper Authentication vulnerability in WPDeveloper Essential Addons for Elementor allows Privilege Escalation. This issue affects Essential Addons for Elementor: from 5.4.0 through 5.7.1.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0852	Buffer overflow in the Address Book of Mobile Device function of Office / Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe.	9.8	More Details
CVE-2023-30353	Shenzen Tenda Technology IP Camera CP3 V11.10.00.2211041355 allows unauthenticated remote code execution via an XML document.	9.8	More Details
CVE-2023-30354	Shenzen Tenda Technology IP Camera CP3 V11.10.00.2211041355 does not defend against physical access to U-Boot via the UART: the Wi-Fi password is shown, and the hardcoded boot password can be inserted for console access.	9.8	More Details
CVE-2022-36937	HHVM 4.172.0 and all prior versions use TLS 1.0 for secure connections when handling tls:// URLs in the stream extension. TLS1.0 has numerous published vulnerabilities and is deprecated. HHVM 4.153.4, 4.168.2, 4.169.2, 4.170.2, 4.171.1, 4.172.1, 4.173.0 replaces TLS1.0 with TLS1.3. Applications that call stream_socket_server or stream_socket_client functions with a URL starting with tls:// are affected.	9.8	More Details
CVE-2023-30194	Prestashop posstaticfooter <= 1.0.0 is vulnerable to SQL Injection via posstaticfooter::getPosCurrentHook().	9.8	More Details
CVE-2022-29842	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability that could allow an attacker to execute code in the context of the root user on a vulnerable CGI file was discovered in Western Digital My Cloud OS 5 devicesThis issue affects My Cloud OS 5: before 5.26.119.	9.8	More Details
CVE-2023-2645	A vulnerability, which was classified as critical, was found in USR USR-G806 1.0.41. Affected is an unknown function of the component Web Management Page. The manipulation of the argument username/password with the input root leads to use of hard-coded password. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to change the configuration settings. VDB-228774 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31475	An issue was discovered on GL.iNet devices before 3.216. The function guci2_get() found in libglutil.so has a buffer overflow when an item is requested from a UCI context, and the value is pasted into a char pointer to a buffer without checking the size of the buffer.	9.8	More Details
CVE-2023-31498	A privilege escalation issue was found in PHP Gurukul Hospital Management System In v.4.0 allows a remote attacker to execute arbitrary code and access sensitive information via the session token parameter.	9.8	More Details
CVE-2023-30330	SoftExpert (SE) Excellence Suite 2.x versions before 2.1.3 is vulnerable to Local File Inclusion in the function /se/v42300/generic/gn_defaultframe/2.0/defaultframe_filter.php.	9.8	More Details
CVE-2023-0851	Buffer overflow in CPCA Resource Download process of Office / Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe.	9.8	More Details
CVE-2023-0853	Buffer overflow in mDNS NSEC record registering process of Office / Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0854	Buffer overflow in NetBIOS QNAME registering and communication process of Office / Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe.	9.8	More Details
CVE-2023-0855	Buffer overflow in IPP number-up attribute process of Office / Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe.	9.8	More Details
CVE-2023-0856	Buffer overflow in IPP sides attribute process of Office / Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe.	9.8	More Details
CVE-2023-29863	Medical Systems Co. Medisys Weblab Products v19.4.03 was discovered to contain a SQL injection vulnerability via the tem:statement parameter in the WSDL files.	9.8	More Details
CVE-2022-47129	PHPOK v6.3 was discovered to contain a remote code execution (RCE) vulnerability.	9.8	More Details
CVE-2023-24540	Not all valid JavaScript whitespace characters are considered to be whitespace. Templates containing whitespace characters outside of the character set "\t\n\f\r\u0020\u2028\u2029" in JavaScript contexts that also contain actions may not be properly sanitized during execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30192	Prestashop possearchproducts 1.7 is vulnerable to SQL Injection via PosSearch::find().	9.8	More Details
CVE-2023-29809	SQL injection vulnerability found in Maximilian Vogt companymaps (cmaps) v.8.0 allows a remote attacker to execute arbitrary code via a crafted script in the request.	9.8	More Details
CVE-2023-30189	Prestashop posstaticblocks <= 1.0.0 is vulnerable to SQL Injection via posstaticblocks::getPosCurrentHook().	9.8	More Details
CVE-2023-1834	Rockwell Automation was made aware that Kinetix 5500 drives, manufactured between May 2022 and January 2023, and are running v7.13 may have the telnet and FTP ports open by default. This could potentially allow attackers unauthorized access to the device through the open ports.	9.4	More Details
CVE-2023-31149	An Improper Input Validation vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to execute arbitrary code. See SEL Service Bulletin dated 2022-11-15 for more details.	9.1	More Details
CVE-2023-31148	An Improper Input Validation vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to execute arbitrary code. See SEL Service Bulletin dated 2022-11-15 for more details.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32080	Wings is the server control plane for Pterodactyl Panel. A vulnerability affecting versions prior to 1.7.5 and versions 1.11.0 prior to 1.11.6 impacts anyone running the affected versions of Wings. This vulnerability can be used to gain access to the host system running Wings if a user is able to modify an server's install script or the install script executes code supplied by the user (either through environment variables, or commands that execute commands based off of user data). This vulnerability has been resolved in version `v1.11.6` of Wings, and has been back-ported to the 1.7 release series in `v1.7.5`. Anyone running `v1.11.x` should upgrade to `v1.11.6` and anyone running `v1.7.x` should upgrade to `v1.7.5`. There are no workarounds aside from upgrading. Running Wings with a rootless container runtime may mitigate the severity of any attacks, however the majority of users are using container runtimes that run as root as per the Wings documentation. SELinux may prevent attackers from performing certain operations against the host system, however privileged containers have a lot of freedom even on systems with SELinux enabled. It should be noted that this was a known attack vector, for attackers to easily exploit this attack it would require compromising an administrator account on a Panel. However, certain eggs (the data structure that holds the install scripts that get passed to Wings) have an issue where they are unknowingly executing shell commands with escalated privileges provided by untrusted user data.	9.0	More Details
CVE-2023-32070	XWiki Platform is a generic wiki platform. Prior to version 14.6-rc-1, HTML rendering didn't check for dangerous attributes/attribute values. This allowed cross-site scripting (XSS) attacks via attributes and link URLs, e.g., supported in XWiki syntax. This has been patched in XWiki 14.6-rc-1. There are no known workarounds apart from upgrading to a fixed version.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-47379	An authenticated, remote attacker may use a out-of-bounds write vulnerability in multiple CODESYS products in multiple versions to write data into memory which can lead to a denial-of-service condition, memory overwriting, or remote code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47386	An authenticated, remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution.	8.8	More Details
CVE-2022-47381	An authenticated remote attacker may use a stack based out-of-bounds write vulnerability in multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution.	8.8	More Details
CVE-2022-47382	An authenticated remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution.	8.8	More Details
CVE-2023-2726	Inappropriate implementation in WebApp Installs in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a malicious web app to bypass install dialog via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-2725	Use after free in Guest View in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-2724	Type confusion in V8 in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-2723	Use after free in DevTools in Google Chrome prior to 113.0.5672.126 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-2722	Use after free in Autofill UI in Google Chrome on Android prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-2721	Use after free in Navigation in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47383	An authenticated, remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution.	8.8	More Details
CVE-2022-47384	An authenticated remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution.	8.8	More Details
CVE-2023-32998	A cross-site request forgery (CSRF) vulnerability in Jenkins AppSpider Plugin 1.0.15 and earlier allows attackers to connect to an attacker-specified URL and send an HTTP POST request with a JSON payload consisting of attacker-specified credentials.	8.8	More Details
CVE-2022-47385	An authenticated, remote attacker may use a stack based out-of-bounds write vulnerability in the CmpAppForce Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution.	8.8	More Details
CVE-2023-32997	Jenkins CAS Plugin 1.6.2 and earlier does not invalidate the previous session on login.	8.8	More Details
CVE-2023-32995	A cross-site request forgery (CSRF) vulnerability in Jenkins SAML Single Sign On(SSO) Plugin 2.0.0 and earlier allows attackers to send an HTTP POST request with JSON body containing attacker-specified content, to miniOrange's API for sending emails.	8.8	More Details
CVE-2023-29930	An issue was found in Genesys CIC Polycom phone provisioning TFTP Server all version allows a remote attacker to execute arbitrary code via the login crednetials to the TFTP server configuration page.	8.8	More Details
CVE-2023-32992	Missing permission checks in Jenkins SAML Single Sign On(SSO) Plugin 2.0.2 and earlier allow attackers with Overall/Read permission to send an HTTP request to an attacker-specified URL and parse the response as XML, or parse a local file on the Jenkins controller as XML.	8.8	More Details
CVE-2023-32991	A cross-site request forgery (CSRF) vulnerability in Jenkins SAML Single Sign On(SSO) Plugin 2.0.2 and earlier allows attackers to send an HTTP request to an attacker-specified URL and parse the response as XML, or parse a local file on the Jenkins controller as XML.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31568	Podofo v0.10.0 was discovered to contain a heap buffer overflow via the component PoDoFo::PdfEncryptRC4::PdfEncryptRC4.	8.8	More Details
CVE-2023-31567	Podofo v0.10.0 was discovered to contain a heap buffer overflow via the component PoDoFo::PdfEncryptAESV3::PdfEncryptAESV3.	8.8	More Details
CVE-2023-31566	Podofo v0.10.0 was discovered to contain a heap-use-after-free via the component PoDoFo::PdfEncrypt::IsMetadataEncrypted().	8.8	More Details
CVE-2023-32989	A cross-site request forgery (CSRF) vulnerability in Jenkins Azure VM Agents Plugin 852.v8d35f0960a_43 and earlier allows attackers to connect to an attacker-specified Azure Cloud server using attacker-specified credentials IDs obtained through another method.	8.8	More Details
CVE-2023-32987	A cross-site request forgery (CSRF) vulnerability in Jenkins Reverse Proxy Auth Plugin 1.7.4 and earlier allows attackers to connect to an attacker-specified LDAP server using attacker-specified credentials.	8.8	More Details
CVE-2023-32986	Jenkins File Parameter Plugin 285.v757c5b_67a_c25 and earlier does not restrict the name (and resulting uploaded file name) of Stashed File Parameters, allowing attackers with Item/Configure permission to create or replace arbitrary files on the Jenkins controller file system with attacker-specified content.	8.8	More Details
CVE-2022-47387	An authenticated remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution.	8.8	More Details
CVE-2022-47388	An authenticated, remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution.	8.8	More Details
CVE-2022-47389	An authenticated, remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32981	An arbitrary file write vulnerability in Jenkins Pipeline Utility Steps Plugin 2.15.2 and earlier allows attackers able to provide crafted archives as parameters to create or replace arbitrary files on the agent file system with attacker-specified content.	8.8	More Details
CVE-2023-31576	An arbitrary file upload vulnerability in Serendipity 2.4-beta1 allows attackers to execute arbitrary code via a crafted HTML or Javascript file.	8.8	More Details
CVE-2022-47380	An authenticated remote attacker may use a stack based out-of-bounds write vulnerability in multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution.	8.8	More Details
CVE-2022-47390	An authenticated, remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution.	8.8	More Details
CVE-2023-32305	aiven-extras is a PostgreSQL extension. Versions prior to 1.1.9 contain a privilege escalation vulnerability, allowing elevation to superuser inside PostgreSQL databases that use the aiven-extras package. The vulnerability leverages missing schema qualifiers on privileged functions called by the aiven-extras extension. A low privileged user can create objects that collide with existing function names, which will then be executed instead. Exploiting this vulnerability could allow a low privileged user to acquire `superuser` privileges, which would allow full, unrestricted access to all data and database functions. And could lead to arbitrary code execution or data access on the underlying host as the `postgres` user. The issue has been patched as of version 1.1.9.	8.8	More Details
CVE-2023-28410	Improper restriction of operations within the bounds of a memory buffer in some Intel(R) i915 Graphics drivers for linux before kernel version 6.2.10 may allow an authenticated user to potentially enable escalation of privilege via local access.	8.8	More Details
CVE-2023-32073	WWBN AVideo is an open source video platform. In versions 12.4 and prior, a command injection vulnerability exists at `plugin/CloneSite/cloneClient.json.php` which allows Remote Code Execution if you CloneSite Plugin. This is a bypass to the fix for CVE-2023-30854, which affects WWBN AVideo up to version 12.3. This issue is patched in commit 1df4af01f80d56ff2c4c43b89d0bac151e7fb6e3.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2457	Out of bounds write in ChromeOS Audio Server in Google Chrome on ChromeOS prior to 113.0.5672.114 allowed a remote attacker to potentially exploit heap corruption via crafted audio file. (Chromium security severity: High)	8.8	More Details
CVE-2023-2458	Use after free in ChromeOS Camera in Google Chrome on ChromeOS prior to 113.0.5672.114 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via UI interaction. (Chromium security severity: High)	8.8	More Details
CVE-2023-27563	The n8n package 0.218.0 for Node.js allows Escalation of Privileges.	8.8	More Details
CVE-2021-34076	File Upload vulnerability in PHPOK 5.7.140 allows remote attackers to run arbitrary code and gain escalated privileges via crafted zip file upload.	8.8	More Details
CVE-2023-32306	Time Tracker is an open source time tracking system. A time-based blind injection vulnerability existed in Time Tracker reports in versions prior to 1.22.13.5792. This was happening because the `reports.php` page was not validating all parameters in POST requests. Because some parameters were not checked, it was possible to craft POST requests with malicious SQL for Time Tracker database. This issue is fixed in version 1.22.13.5792. As a workaround, use the fixed code in `ttReportHelper.class.php` from version 1.22.13.5792.	8.8	More Details
CVE-2023-20877	VMware Aria Operations contains a privilege escalation vulnerability. An authenticated malicious user with ReadOnly privileges can perform code execution leading to privilege escalation.	8.8	More Details
CVE-2023-27298	Uncontrolled search path in the WULT software maintained by Intel(R) before version 1.0.0 (commit id 592300b) may allow an unauthenticated user to potentially enable escalation of privilege via network access.	8.8	More Details
CVE-2023-27889	Cross-site request forgery (CSRF) vulnerability in LIQUID SPEECH BALLOON versions prior to 1.2 allows a remote unauthenticated attacker to hijack the authentication of a user and to perform unintended operations by having a user view a malicious page.	8.8	More Details
CVE-2022-41784	Improper access control in kernel mode driver for the Intel(R) OFU software before version 14.1.30 may allow an authenticated user to potentially enable escalation of privilege via local access	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30130	An issue found in CraftCMS v.3.8.1 allows a remote attacker to execute arbitrary code via a crafted script to the Section parameter.	8.8	More Details
CVE-2023-31528	Motorola CX2L Router 1.0.1 was discovered to contain a command injection vulnerability via the staticroute_list parameter.	8.8	More Details
CVE-2023-31529	Motorola CX2L Router 1.0.1 was discovered to contain a command injection vulnerability via the system_time_timezone parameter.	8.8	More Details
CVE-2023-31530	Motorola CX2L Router 1.0.1 was discovered to contain a command injection vulnerability via the smartqos_priority_devices parameter.	8.8	More Details
CVE-2023-31531	Motorola CX2L Router 1.0.1 was discovered to contain a command injection vulnerability via the tomography_ping_number parameter.	8.8	More Details
CVE-2023-29657	eXtplorer 2.1.15 is vulnerable to Insecure Permissions. File upload in file manager allows uploading zip file containing php pages with arbitrary code executions.	8.8	More Details
CVE-2020-13378	Loadbalancer.org Enterprise VA MAX through 8.3.8 has an OS Command Injection vulnerability that allows a remote authenticated attacker to execute arbitrary code.	8.8	More Details
CVE-2023-31572	An issue in Bludit 4.0.0-rc-2 allows authenticated attackers to change the Administrator password and escalate privileges via a crafted request.	8.8	More Details
CVE-2023-22441	Missing authentication for critical function exists in Seiko Solutions SkyBridge series, which may allow a remote attacker to obtain or alter the setting information of the product or execute some critical functions without authentication, e.g., rebooting the product. Affected products and versions are as follows: SkyBridge MB-A200 firmware Ver. 01.00.05 and earlier, and SkyBridge BASIC MB-A130 firmware Ver. 1.4.1 and earlier	8.6	More Details
CVE-2022-41985	An authentication bypass vulnerability exists in the Authentication functionality of Weston Embedded uC-FTPs v 1.98.00. A specially crafted set of network packets can lead to authentication bypass and denial of service. An attacker can send a sequence of unauthenticated packets to trigger this vulnerability.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21804	Out-of-bounds write in software for the Intel QAT Driver for Windows before version 1.9.0-0008 may allow an authenticated user to potentially enable escalation of privilege via local access.	8.4	More Details
CVE-2023-25568	Boxo, formerly known as go-libipfs, is a library for building IPFS applications and implementations. In versions 0.4.0 and 0.5.0, if an attacker is able allocate arbitrary many bytes in the Bitswap server, those allocations are lasting even if the connection is closed. This affects users accepting untrusted connections with the Bitswap server and also affects users using the old API stubs at `github.com/ipfs/go-libipfs/bitswap` because users then transitively import `github.com/ipfs/go-libipfs/bitswap/server`. Boxo versions 0.6.0 and 0.4.1 contain a patch for this issue. As a workaround, those who are using the stub object at `github.com/ipfs/go-libipfs/bitswap` not taking advantage of the features provided by the server can refactor their code to use the new split API that will allow them to run in a client only mode: `github.com/ipfs/go-libipfs/bitswap/client`.	8.2	More Details
CVE-2023-25545	Improper buffer restrictions in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable escalation of privilege via local access.	8.2	More Details
CVE-2022-41699	Incorrect permission assignment for critical resource in some Intel(R) QAT drivers for Windows before version 1.9.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2023-32308	anuko timetracker is an open source time tracking system. Boolean-based blind SQL injection vulnerability existed in Time Tracker invoices.php in versions prior to 1.22.11.5781. This was happening because of a coding error after validating parameters in POST requests. There was no check for errors before adjusting invoice sorting order. Because of this, it was possible to craft a POST request with malicious SQL for Time Tracker database. This issue has been fixed in version 1.22.11.5781. Users are advised to upgrade. Users unable to upgrade may insert an additional check for errors in a condition before calling `ttGroupHelper::getActiveInvoices()` in invoices.php.	8.2	More Details
CVE-2022-40207	Improper access control in the Intel(R) SUR software before version 2.4.8989 may allow an authenticated user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2023-22661	Buffer overflow in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable escalation of privilege via local access.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22297	Access of memory location after end of buffer in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable escalation of privilege via local access.	8.2	More Details
CVE-2022-44619	Insecure storage of sensitive information in the Intel(R) DCM software before version 5.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2023-32955	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in DHCP Client Functionality in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows man-in-the-middle attackers to execute arbitrary commands via unspecified vectors.	8.1	More Details
CVE-2020-13377	The web-services interface of Loadbalancer.org Enterprise VA MAX through 8.3.8 could allow an authenticated, remote, low-privileged attacker to conduct directory traversal attacks and obtain read and write access to sensitive files.	8.1	More Details
CVE-2023-29032	An attacker that has gained access to certain private information can use this to act as other user. Vendor: The Apache Software Foundation Versions Affected: Apache OpenMeetings from 3.1.3 before 7.1.0	8.1	More Details
CVE-2023-31150	A Storing Passwords in a Recoverable Format vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) database system could allow an authenticated attacker to retrieve passwords. See SEL Service Bulletin dated 2022-11-15 for more details.	8.0	More Details
CVE-2022-29841	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that was caused by a command that read files from a privileged location and created a system command without sanitizing the read data. This command could be triggered by an attacker remotely to cause code execution and gain a reverse shell in Western Digital My Cloud OS 5 devices.This issue affects My Cloud OS 5: before 5.26.119.	8.0	More Details
CVE-2023-22442	Out of bounds write in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable escalation of privilege via local access.	7.9	More Details
CVE-2023-21110	In several functions of SnoozeHelper.java, there is a possible way to grant notifications access due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258422365	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2124	An out-of-bounds memory access flaw was found in the Linux kernel's XFS file system in how a user restores an XFS image after failure (with a dirty log journal). This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.8	More Details
CVE-2023-29283	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-29282	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-27385	Heap-based buffer overflow vulnerability exists in CX-Drive All models all versions. By having a user open a specially crafted SDD file, arbitrary code may be executed and/or information may be disclosed.	7.8	More Details
CVE-2023-29281	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-29280	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-29278	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-25428	A DLL Hijacking issue discovered in Soft-o Free Password Manager 1.1.20 allows attackers to create arbitrary DLLs leading to code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21117	In registerReceiverWithFeature of ActivityManagerService.java, there is a possible way for isolated processes to register a broadcast receiver due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-263358101	7.8	More Details
CVE-2023-29284	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-29276	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-29285	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-29274	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-29273	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-21109	In multiple places of AccessibilityService, there is a possible way to hide the app from the user due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261589597	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21107	In retrieveAppEntry of NotificationAccessDetails.java, there is a missing permission check. This could lead to local escalation of privilege across user boundaries with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-259385017	7.8	More Details
CVE-2023-21106	In adreno_set_param of adreno_gpu.c, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-265016072References: Upstream kernel	7.8	More Details
CVE-2023-21102	In __efi_rt_asm_wrapper of efi-rt-wrapper.S, there is a possible bypass of shadow stack protection due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-260821414References: Upstream kernel	7.8	More Details
CVE-2023-31497	Incorrect access control in Quick Heal Technologies Limited Seqrite Endpoint Security (EPS) all versions prior to v8.0 allows attackers to escalate privileges to root via supplying a crafted binary to the target system.	7.8	More Details
CVE-2023-23569	Stack-based buffer overflow for some Intel(R) Trace Analyzer and Collector software before version 2021.8.0 published Dec 2022 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2023-29275	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-2629	Improper Neutralization of Formula Elements in a CSV File in GitHub repository pimcore/customer-data-framework prior to 3.3.9.	7.8	More Details
CVE-2023-31906	Jerryscript 3.0.0(commit 1a2c047) was discovered to contain a heap-buffer-overflow via the component lexer_compare_identifier_to_chars at /jerry-core/parser/js/js-lexer.c.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25006	A malicious actor may convince a user to open a malicious USD file that may trigger a use-after-free vulnerability which could result in code execution.	7.8	More Details
CVE-2023-25007	A malicious actor may convince a user to open a malicious USD file that may trigger an uninitialized pointer which could result in code execution.	7.8	More Details
CVE-2023-25008	A malicious actor may convince a user to open a malicious USD file that may trigger an out-of-bounds read vulnerability which could result in code execution.	7.8	More Details
CVE-2023-25009	A malicious actor may convince a user to open a malicious USD file that may trigger an out-of-bounds write vulnerability which could result in code execution.	7.8	More Details
CVE-2023-31910	Jerryscript 3.0 (commit 05dbbd1) was discovered to contain a heap-buffer-overflow via the component parser_parse_function_statement at /jerry-core/parser/js/js-parser-statm.c.	7.8	More Details
CVE-2022-29919	Use after free in the Intel(R) VROC software before version 7.7.6.1003 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2023-31908	Jerryscript 3.0 (commit 05dbbd1) was discovered to contain a heap-buffer-overflow via the component ecma_builtin_typedarray_prototype_sort.	7.8	More Details
CVE-2023-25005	A maliciously crafted DLL file can be forced to read beyond allocated boundaries in Autodesk InfraWorks 2023, and 2021 when parsing the DLL files could lead to a resource injection vulnerability.	7.8	More Details
CVE-2023-31907	Jerryscript 3.0.0 was discovered to contain a heap-buffer-overflow via the component scanner_literal_is_created at /jerry-core/parser/js/js-scanner-util.c.	7.8	More Details
CVE-2023-30768	Improper access control in the Intel(R) Server Board S2600WTT belonging to the Intel(R) Server Board S2600WT Family with the BIOS version 0016 may allow a privileged user to potentially enable escalation of privilege via local access.	7.7	More Details
CVE-2022-4048	Inadequate Encryption Strength in CODESYS Development System V3 versions prior to V3.5.18.40 allows an unauthenticated local attacker to access and manipulate code of the encrypted boot application.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31199	Improper access control in the Intel(R) Solid State Drive Toolbox(TM) before version 3.4.5 may allow a privileged user to potentially enable escalation of privilege via local access.	7.7	More Details
CVE-2023-31477	A path traversal issue was discovered on GL.iNet devices before 3.216. Through the file sharing feature, it is possible to share an arbitrary directory, such as /tmp or /etc, because there is no server-side restriction to limit sharing to the USB path.	7.5	More Details
CVE-2023-2443	Rockwell Automation ThinManager product allows the use of medium strength ciphers. If the client requests an insecure cipher, a malicious actor could potentially decrypt traffic sent between the client and server API.	7.5	More Details
CVE-2023-30351	Shenzen Tenda Technology IP Camera CP3 V11.10.00.2211041355 was discovered to contain a hard-coded default password for root which is stored using weak encryption. This vulnerability allows attackers to connect to the TELNET service (or UART) by using the exposed credentials.	7.5	More Details
CVE-2023-31146	Vyper is a Pythonic smart contract language for the Ethereum virtual machine. Prior to version 0.3.8, during codegen, the length word of a dynarray is written before the data, which can result in out-of-bounds array access in the case where the dynarray is on both the lhs and rhs of an assignment. The issue can cause data corruption across call frames. The expected behavior is to revert due to out-of-bounds array access. Version 0.3.8 contains a patch for this issue.	7.5	More Details
CVE-2023-30356	Missing Support for an Integrity Check in Shenzen Tenda Technology IP Camera CP3 V11.10.00.2211041355 allows attackers to update the device with crafted firmware	7.5	More Details
CVE-2023-29790	kodbox 1.2.x through 1.3.7 has a Sensitive Information Leakage issue.	7.5	More Details
CVE-2023-32058	Vyper is a Pythonic smart contract language for the Ethereum virtual machine. Prior to version 0.3.8, due to missing overflow check for loop variables, by assigning the iterator of a loop to a variable, it is possible to overflow the type of the latter. The issue seems to happen only in loops of type `for i in range(a, a + N)` as in loops of type `for i in range(start, stop)` and `for i in range(stop)`, the compiler is able to raise a `TypeMismatch` when trying to overflow the variable. The problem has been patched in version 0.3.8.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31677	Insecure permissions in luowice 3.5.18 allow attackers to view information for other alarm devices via modification of the eseeid parameter.	7.5	More Details
CVE-2021-45345	Buffer Overflow vulnerability found in En3rgy WebcamServer v.0.5.2 allows a remote attacker to cause a denial of service via the WebcamServer.exe file.	7.5	More Details
CVE-2023-2665	Storage of Sensitive Data in a Mechanism without Access Control in GitHub repository francoisjacquet/rosariosis prior to 11.0.	7.5	More Details
CVE-2023-33000	Jenkins NS-ND Integration Performance Publisher Plugin 4.8.0.149 and earlier does not mask credentials displayed on the configuration form, increasing the potential for attackers to observe and capture them.	7.5	More Details
CVE-2023-28356	A vulnerability has been identified where a maliciously crafted message containing a specific chain of characters can cause the chat to enter a hot loop on one of the processes, consuming ~120% CPU and rendering the service unresponsive.	7.5	More Details
CVE-2023-33001	Jenkins HashiCorp Vault Plugin 360.v0a_1c04cf807d and earlier does not properly mask (i.e., replace with asterisks) credentials in the build log when push mode for durable task logging is enabled.	7.5	More Details
CVE-2023-2666	Allocation of Resources Without Limits or Throttling in GitHub repository froxlor/froxlor prior to 2.0.16.	7.5	More Details
CVE-2023-27564	The n8n package 0.218.0 for Node.js allows Information Disclosure.	7.5	More Details
CVE-2023-31442	In Lightbend Akka before 2.8.1, the async-dns resolver (used by Discovery in DNS mode and transitively by Cluster Bootstrap) uses predictable DNS transaction IDs when resolving DNS records, making DNS resolution subject to poisoning by an attacker. If the application performing discovery does not validate (e.g., via TLS) the authenticity of the discovered service, this may result in exfiltration of application data (e.g., persistence events may be published to an unintended Kafka broker). If such validation is performed, then the poisoning constitutes a denial of access to the intended service. This affects Akka 2.5.14 through 2.8.0, and Akka Discovery through 2.8.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30172	A directory traversal vulnerability in the /get-artifact API method of the mlflow platform up to v2.0.1 allows attackers to read arbitrary files on the server via the path parameter.	7.5	More Details
CVE-2023-32059	Vyper is a Pythonic smart contract language for the Ethereum virtual machine. Prior to version 0.3.8, internal calls with default arguments are compiled incorrectly. Depending on the number of arguments provided in the call, the defaults are added not right-to-left, but left-to-right. If the types are incompatible, typechecking is bypassed. The ability to pass kwargs to internal functions is an undocumented feature that is not well known about. The issue is patched in version 0.3.8.	7.5	More Details
CVE-2023-31679	Incorrect access control in Videogo v6.8.1 allows attackers to access images from other devices via modification of the Device Id parameter.	7.5	More Details
CVE-2023-31623	An issue in the mp_box_copy component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-2180	The KIWIZ Invoices Certification & PDF System WordPress plugin through 2.1.3 does not validate the path of files to be downloaded, which could allow unauthenticated attacker to read/downlaod arbitrary files, as well as perform PHAR unserialization (assuming they can upload a file on the server)	7.5	More Details
CVE-2022-34147	Improper input validation in BIOS firmware for some Intel(R) NUC 9 Extreme Laptop Kits, Intel(R) NUC Performance Kits, Intel(R) NUC Performance Mini PC, Intel(R) NUC 8 Compute Element, Intel(R) NUC Pro Kit, Intel(R) NUC Pro Board, and Intel(R) NUC Compute Element may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2022-33894	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.	7.5	More Details
CVE-2022-28699	Improper input validation for some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2022-47391	In multiple CODESYS products in multiple versions an unauthorized, remote attacker may use a improper input validation vulnerability to read from invalid addresses leading to a denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31617	An issue in the dk_set_delete component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31622	An issue in the sqlc_make_policy_trig component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-23445	Improper Access Control in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows an unprivileged remote attacker to gain unauthorized access to data fields by using a therefore unpriviledged account via the REST interface.	7.5	More Details
CVE-2023-31621	An issue in the kc_var_col component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31620	An issue in the dv_compare component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-23446	Improper Access Control in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows an unprivileged remote attacker to download files by using a therefore unpriviledged account via the REST interface.	7.5	More Details
CVE-2023-31626	An issue in the gpf_notice component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-23447	Uncontrolled Resource Consumption in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows an unprivileged remote attacker to influence the availability of the webserver by invocing several open file requests via the REST interface.	7.5	More Details
CVE-2023-0812	The Active Directory Integration / LDAP Integration WordPress plugin before 4.1.1 does not have proper authorization or nonce values for some POST requests, leading to unauthenticated data disclosure.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27510	JB Inquiry form contains an exposure of private personal information to an unauthorized actor vulnerability, which may allow a remote unauthenticated attacker to obtain information entered from forms created using the affected product. The affected products and versions are as follows: JB Inquiry form versions 0.6.1 and 0.6.0, JB Inquiry form versions 0.5.2, 0.5.1 and 0.5.0, and JB Inquiry form version 0.40.	7.5	More Details
CVE-2022-36339	Improper input validation in firmware for Intel(R) NUC 8 Compute Element, Intel(R) NUC 11 Compute Element, Intel(R) NUC 12 Compute Element may allow a privileged user to enable escalation of privilege via local access.	7.5	More Details
CVE-2023-27527	Shinseiyo Sogo Soft (7.9A) and earlier improperly restricts XML external entity references (XXE). By processing a specially crafted XML file, arbitrary files on the PC may be accessed by an attacker.	7.5	More Details
CVE-2023-31619	An issue in the sch_name_to_object component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31607	An issue in the __libc_malloc component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31608	An issue in the artm_div_int component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31609	An issue in the dfe_unit_col_loci component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31610	An issue in the _IO_default_xsputn component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31611	An issue in the __libc_longjmp component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31612	An issue in the dfe_qexp_list component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31618	An issue in the sqlc_union_dt_wrap component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31613	An issue in the __nss_database_lookup component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31627	An issue in the strhash component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31614	An issue in the mp_box_deserialize_string function in openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement.	7.5	More Details
CVE-2023-31615	An issue in the chash_array component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-22318	Denial of service in Webconf in Tribe29 Checkmk Appliance before 1.6.5.	7.5	More Details
CVE-2023-31616	An issue in the bif_mod component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-32784	In KeePass 2.x before 2.54, it is possible to recover the cleartext master password from a memory dump, even when a workspace is locked or no longer running. The memory dump can be a KeePass process dump, swap file (pagefile.sys), hibernation file (hiberfil.sys), or RAM dump of the entire system. The first character cannot be recovered. In 2.54, there is different API usage and/or random string insertion for mitigation.	7.5	More Details
CVE-2023-32758	giturlparse (aka git-url-parse) through 1.2.2, as used in Semgrep 1.5.2 through 1.24.1, is vulnerable to ReDoS (Regular Expression Denial of Service) if parsing untrusted URLs. This might be relevant if Semgrep is analyzing an untrusted package (for example, to check whether it accesses any Git repository at an http:// URL), and that package's author placed a ReDoS attack payload in a URL used by the package.	7.5	More Details
CVE-2023-31631	An issue in the sqlo_preds_contradiction component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32787	The OPC UA Legacy Java Stack before 6f176f2 enables an attacker to block OPC UA server applications via uncontrolled resource consumption so that they can no longer serve client applications.	7.5	More Details
CVE-2023-32309	PyMdown Extensions is a set of extensions for the `Python-Markdown` markdown project. In affected versions an arbitrary file read is possible when using include file syntax. By using the syntax `--8<--"/etc/passwd"` or `--8<--"/proc/self/environ"` the content of these files will be rendered in the generated documentation. Additionally, a path relative to a specified, allowed base path can also be used to render the content of a file outside the specified base paths: `--8<-- "../../../../etc/passwd"`. Within the Snippets extension, there exists a `base_path` option but the implementation is vulnerable to Directory Traversal. The vulnerable section exists in `get_snippet_path(self, path)` lines 155 to 174 in snippets.py. Any readable file on the host where the plugin is executing may have its content exposed. This can impact any use of Snippets that exposes the use of Snippets to external users. It is never recommended to use Snippets to process user-facing, dynamic content. It is designed to process known content on the backend under the control of the host, but if someone were to accidentally enable it for user-facing content, undesired information could be exposed. This issue has been addressed in version 10.0. Users are advised to upgrade. Users unable to upgrade may restrict relative paths by filtering input.	7.5	More Details
CVE-2023-23444	Missing Authentication for Critical Function in SICK Flexi Classic and Flexi Soft Gateways with Partnumbers 1042193, 1042964, 1044078, 1044072, 1044073, 1044074, 1099830, 1099832, 1127717, 1069070, 1112296, 1051432, 1102420, 1127487, 1121596, 1121597 allows an unauthenticated remote attacker to influence the availability of the device by changing the IP settings of the device via broadcasted UDP packets.	7.5	More Details
CVE-2022-43507	Improper buffer restrictions in the Intel(R) QAT Engine for OpenSSL before version 0.6.16 may allow a privileged user to potentially enable escalation of privilege via network access.	7.5	More Details
CVE-2022-47879	A Remote Code Execution (RCE) vulnerability in /be/rpc.php in Jedox 2020.2.5 allows remote authenticated users to load arbitrary PHP classes from the 'rtn' directory and execute its methods.	7.5	More Details
CVE-2023-31922	QuickJS commit 2788d71 was discovered to contain a stack-overflow via the component js_proxy_isArray at quickjs.c.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31630	An issue in the sqlo_query_spec component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-23578	Improper access control vulnerability in SkyBridge MB-A200 firmware Ver. 01.00.05 and earlier allows a remote unauthenticated attacker to connect to the product's ADB port.	7.5	More Details
CVE-2023-23906	Missing authentication for critical function exists in SkyBridge MB-A100/110 firmware Ver. 4.2.0 and earlier, which may allow a remote unauthenticated attacker to execute some critical functions without authentication, e.g., rebooting the product.	7.5	More Details
CVE-2023-31629	An issue in the sqlo_union_scope component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31624	An issue in the sinv_check_exp component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31625	An issue in the psiginfo component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-31628	An issue in the stricmp component of openlink virtuoso-opensource v7.2.9 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2023-26126	All versions of the package m.static are vulnerable to Directory Traversal due to improper input sanitization of the path being requested via the requestFile function.	7.5	More Details
CVE-2023-25072	Use of weak credentials exists in SkyBridge MB-A100/110 firmware Ver. 4.2.0 and earlier, which may allow a remote unauthenticated attacker to decrypt password for the WebUI of the product.	7.5	More Details
CVE-2023-25184	Use of weak credentials exists in Seiko Solutions SkyBridge and SkySpider series, which may allow a remote unauthenticated attacker to decrypt password for the WebUI of the product. Affected products and versions are as follows: SkyBridge MB-A200 firmware Ver. 01.00.05 and earlier, SkyBridge BASIC MB-A130 firmware Ver. 1.4.1 and earlier, and SkySpider MB-R210 firmware Ver. 1.01.00 and earlier.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31131	Greenplum Database (GPDB) is an open source data warehouse based on PostgreSQL. In versions prior to 6.22.3 Greenplum Database used an unsafe methods to extract tar files within GPPKGs. greenplum-db is vulnerable to path traversal leading to arbitrary file writes. An attacker can use this vulnerability to overwrite data or system files potentially leading to crash or malfunction of the system. Any files which are accessible to the running process are at risk. All users are requested to upgrade to Greenplum Database version 6.23.2 or higher. There are no known workarounds for this vulnerability.	7.4	More Details
CVE-2023-24539	Angle brackets (<>) are not considered dangerous characters when inserted into CSS contexts. Templates containing multiple actions separated by a '/' character can result in unexpectedly closing the CSS context and allowing for injection of unexpected HTML, if executed with untrusted input.	7.3	More Details
CVE-2023-29400	Templates containing actions in unquoted HTML attributes (e.g. "attr={{.}}") executed with empty input can result in output with unexpected results when parsed due to HTML normalization rules. This may allow injection of arbitrary attributes into tags.	7.3	More Details
CVE-2023-2641	A vulnerability was found in SourceCodester Online Internship Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file admin/login.php of the component POST Parameter Handler. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-228770 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2023-31844	Sourcecodester Faculty Evaluation System v1.0 is vulnerable to SQL Injection via /eval/admin/manage_subject.php?id=.	7.2	More Details
CVE-2022-32766	Improper input validation for some Intel(R) BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	More Details
CVE-2023-2649	A vulnerability was found in Tenda AC23 16.03.07.45_cn. It has been declared as critical. This vulnerability affects unknown code of the file /bin/ate of the component Service Port 7329. The manipulation of the argument v2 leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-228778 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29246	An attacker who has gained access to an admin account can perform RCE via null-byte injection Vendor: The Apache Software Foundation Versions Affected: Apache OpenMeetings from 2.0.0 before 7.1.0	7.2	More Details
CVE-2023-22312	Improper access control for some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	More Details
CVE-2023-30506	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	More Details
CVE-2023-30505	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	More Details
CVE-2023-30504	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	More Details
CVE-2023-30503	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	More Details
CVE-2023-30502	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	More Details
CVE-2023-30501	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20878	VMware Aria Operations contains a deserialization vulnerability. A malicious actor with administrative privileges can execute arbitrary commands and disrupt the system.	7.2	More Details
CVE-2023-31843	Sourcecodester Faculty Evaluation System v1.0 is vulnerable to SQL Injection via /eval/admin/view_faculty.php?id=.	7.2	More Details
CVE-2023-30763	Heap-based overflow in Intel(R) SoC Watch based software before version 2021.1 may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	More Details
CVE-2023-1207	This HTTP Headers WordPress plugin before 1.18.8 has an import functionality which executes arbitrary SQL on the server, leading to an SQL Injection vulnerability.	7.2	More Details
CVE-2023-1549	The Ad Inserter WordPress plugin before 2.7.27 unserializes user input provided via the settings, which could allow high privilege users such as admin to perform PHP Object Injection when a suitable gadget is present	7.2	More Details
CVE-2023-32568	An issue was discovered in Veritas InfoScale Operations Manager (VIOM) before 7.4.2.800 and 8.x before 8.0.410. The VIOM web application does not validate user-supplied data and appends it to OS commands and internal binaries used by the application. An attacker with root/administrator level privileges can leverage this to read sensitive data stored on the servers, modify data or server configuration, and delete data or application configuration.	7.2	More Details
CVE-2023-32569	An issue was discovered in Veritas InfoScale Operations Manager (VIOM) before 7.4.2.800 and 8.x before 8.0.410. The InfoScale VIOM web application is vulnerable to SQL Injection in some of the areas of the application. This allows attackers (who must have admin credentials) to submit arbitrary SQL commands on the back-end database to create, read, update, or delete any sensitive data stored in the database.	7.2	More Details
CVE-2023-31845	Sourcecodester Faculty Evaluation System v1.0 is vulnerable to SQL Injection via /eval/admin/manage_class.php?id=.	7.2	More Details
CVE-2022-42465	Improper access control in kernel mode driver for the Intel(R) OFU software before version 14.1.30 may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	More Details
CVE-2023-31842	Sourcecodester Faculty Evaluation System v1.0 is vulnerable to SQL Injection via /eval/index.php?page=edit_faculty&id=.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31502	Altenergy Power Control Software C1.2.5 was discovered to contain a remote code execution (RCE) vulnerability via the component /models/management_model.php.	7.2	More Details
CVE-2023-30777	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WP Engine Advanced Custom Fields Pro, WP Engine Advanced Custom Fields plugins <= 6.1.5 versions.	7.1	More Details
CVE-2023-27455	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Maui Marketing Update Image Tag Alt Attribute plugin <= 2.4.5 versions.	7.1	More Details
CVE-2023-24392	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution Full Width Banner Slider Wp plugin <= 1.1.7 versions.	7.1	More Details
CVE-2023-27419	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Everest themes Viable Blog theme <= 1.1.4 versions.	7.1	More Details
CVE-2023-29101	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Muffingroup Betheme theme <= 26.7.5 versions.	7.1	More Details
CVE-2023-22706	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in PropertyHive plugin <= 1.5.48 versions.	7.1	More Details
CVE-2022-47590	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Fugu Maintenance Switch plugin <= 1.5.2 versions.	7.1	More Details
CVE-2022-47600	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution Mass Email To users plugin <= 1.1.4 versions.	7.1	More Details
CVE-2023-29439	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in FooPlugins FooGallery plugin <= 2.2.35 versions.	7.1	More Details
CVE-2023-22703	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Webcodin WCP Contact Form plugin <= 3.1.0 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41690	Improper access control in the Intel(R) Retail Edge Mobile iOS application before version 3.4.7 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.1	More Details
CVE-2023-2444	A cross site request forgery vulnerability exists in Rockwell Automation's FactoryTalk Vantagepoint. This vulnerability can be exploited in two ways. If an attacker sends a malicious link to a computer that is on the same domain as the FactoryTalk Vantagepoint server and a user clicks the link, the attacker could impersonate the legitimate user and send requests to the affected product. Additionally, if an attacker sends an untrusted link to a computer that is not on the same domain as the server and a user opens the FactoryTalk Vantagepoint website, enters credentials for the FactoryTalk Vantagepoint server, and clicks on the malicious link a cross site request forgery attack would be successful as well.	7.1	More Details
CVE-2022-47441	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Charitable Donations & Fundraising Team Donation Forms by Charitable plugin <= 1.7.0.10 versions.	7.1	More Details
CVE-2023-29031	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.	7.0	More Details
CVE-2023-29023	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.	7.0	More Details
CVE-2023-29030	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.	7.0	More Details
CVE-2022-40210	Exposure of data element to wrong session in the Intel DCM software before version 5.0.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.8	More Details
CVE-2023-2310	A Channel Accessible by Non-Endpoint vulnerability in the Schweitzer Engineering Laboratories SEL Real-Time Automation Controller (RTAC) could allow a remote attacker to perform a man-in-the-middle (MiTM) that could result in denial of service. See the ACSELERATOR RTAC SEL-5033 Software instruction manual date code 20210915 for more details.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20694	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07733998 / ALPS07874388 (For MT6880 and MT6890 only); Issue ID: ALPS07733998 / ALPS07874388 (For MT6880 and MT6890 only).	6.7	More Details
CVE-2023-20699	In adsp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696073; Issue ID: ALPS07696073.	6.7	More Details
CVE-2023-20700	In widevine, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07643304; Issue ID: ALPS07643304.	6.7	More Details
CVE-2023-20701	In widevine, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07643270; Issue ID: ALPS07643270.	6.7	More Details
CVE-2023-20707	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628556; Issue ID: ALPS07628556.	6.7	More Details
CVE-2023-20708	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07581655; Issue ID: ALPS07581655.	6.7	More Details
CVE-2023-20718	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645181; Issue ID: ALPS07645181.	6.7	More Details
CVE-2023-2514	Mattermost Sever fails to redact the DB username and password before emitting an application log during server initialization.	6.7	More Details
CVE-2023-20721	In isp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07162155; Issue ID: ALPS07162155.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20720	In pqframework, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629586; Issue ID: ALPS07629586.	6.7	More Details
CVE-2023-20722	In m4u, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07771518; Issue ID: ALPS07680084.	6.7	More Details
CVE-2023-29242	Improper access control for Intel(R) oneAPI Toolkits before version 2021.1 Beta 10 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-31197	Uncontrolled search path in the Intel(R) Trace Analyzer and Collector before version 2020 update 3 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-21116	In verifyReplacingVersionCode of InstallPackageHelper.java, there is a possible way to downgrade system apps below system image version due to a logic error in the code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-256202273	6.7	More Details
CVE-2023-20879	VMware Aria Operations contains a Local privilege escalation vulnerability. A malicious actor with administrative privileges in the Aria Operations application can gain root access to the underlying operating system.	6.7	More Details
CVE-2023-20880	VMware Aria Operations contains a privilege escalation vulnerability. A malicious actor with administrative access to the local system can escalate privileges to 'root'.	6.7	More Details
CVE-2023-20696	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07856356 / ALPS07874388 (For MT6880 and MT6890 only); Issue ID: ALPS07856356 / ALPS07874388 (For MT6880 and MT6890 only).	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20695	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734012 / ALPS07874363 (For MT6880, MT6890, MT6980 and MT6990 only); Issue ID: ALPS07734012 / ALPS07874363 (For MT6880, MT6890, MT6980 and MT6990 only).	6.7	More Details
CVE-2023-20673	In vcu, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07519103; Issue ID: ALPS07519103.	6.7	More Details
CVE-2022-34848	Uncontrolled search path for the Intel(R) NUC Pro Software Suite before version 2.0.0.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-33963	Incorrect default permissions in the software installer for Intel(R) Unite(R) Client software for Windows before version 4.2.34870 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-32576	Uncontrolled search path in the Intel(R) Unite(R) Plugin SDK before version 4.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-38101	Uncontrolled search path in some Intel(R) NUC Chaco Canyon BIOS update software before version iFlashV Windows 5.13.00.2105 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-38103	Insecure inherited permissions in the Intel(R) NUC Software Studio Service installer before version 1.17.38.0 may allow an authenticated user to potentially enable escalation of privilege via local access	6.7	More Details
CVE-2023-27386	Uncontrolled search path in some Intel(R) Pathfinder for RISC-V software may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-27382	Incorrect default permissions in the Audio Service for some Intel(R) NUC P14E Laptop Element software for Windows 10 before version 1.0.0.156 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-40971	Incorrect default permissions for the Intel(R) HDMI Firmware Update Tool for NUC before version 1.79.1.1 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-2022-40972	Improper access control in some Intel(R) QAT drivers for Windows before version 1.9.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-30338	Incorrect default permissions in the Intel(R) VROC software before version 7.7.6.1003 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-41628	Uncontrolled search path element in the HotKey Services for some Intel(R) NUC P14E Laptop Element software for Windows 10 before version 1.1.44 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-22440	Incorrect default permissions in the Intel(R) SCS Add-on software installer for Microsoft SCCM all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-22379	Improper input validation in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable information disclosure via local access.	6.7	More Details
CVE-2023-22355	Uncontrolled search path in some Intel(R) oneAPI Toolkit and component software installers before version 4.3.0.251 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-46656	Insecure inherited permissions for the Intel(R) NUC Pro Software Suite before version 2.0.0.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-43474	Uncontrolled search path for the DSP Builder software installer before version 22.4 for Intel(R) FPGAs Pro Edition may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-21162	Uncontrolled search path for the Intel(R) HDMI Firmware Update tool for NUC before version 1.79.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-41998	Uncontrolled search path in the Intel(R) DCM software before version 5.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-41982	Uncontrolled search path element in the Intel(R) VTune(TM) Profiler software before version 2023.0 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-2022-41658	Insecure inherited permissions in the Intel(R) VTune(TM) Profiler software before version 2023.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-41693	Uncontrolled search path in the Intel(R) Quartus(R) Prime Pro edition software before version 22.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-32578	Improper access control for the Intel(R) NUC Pro Software Suite before version 2.0.0.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-41687	Insecure inherited permissions in the HotKey Services for some Intel(R) NUC P14E Laptop Element software for Windows 10 before version 1.1.44 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-34855	Path traversal for the Intel(R) NUC Pro Software Suite before version 2.0.0.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-36391	Incorrect default permissions for the Intel(R) NUC Pro Software Suite before version 2.0.0.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-2548	The RegistrationMagic plugin for WordPress is vulnerable to Insecure Direct Object References in versions up to, and including, 5.2.0.5. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for authenticated attackers, with administrator-level permissions and above, to change user passwords and potentially take over super-administrator accounts in multisite setup.	6.6	More Details
CVE-2023-0007	A cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS software on Panorama appliances enables an authenticated read-write administrator to store a JavaScript payload in the web interface that will execute in the context of another administrator’s browser when viewed.	6.5	More Details
CVE-2022-46378	An out-of-bounds read vulnerability exists in the PORT command parameter extraction functionality of Weston Embedded uC-FTPs v 1.98.00. A specially-crafted set of network packets can lead to denial of service. An attacker can send packets to trigger this vulnerability.This vulnerability occurs when no port argument is provided to the `PORT` command.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23688	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Sumo Social Share Boost plugin <= 4.4 versions.	6.5	More Details
CVE-2023-2512	Prior to version v1.20230419.0, the FormData API implementation was subject to an integer overflow. If a FormData instance contained more than 2^31 elements, the forEach() method could end up reading from the wrong location in memory while iterating over elements. This would most likely lead to a segmentation fault, but could theoretically allow arbitrary undefined behavior. In order for the bug to be exploitable, the process would need to be able to allocate 160GB of RAM. Due to this, the bug was never exploitable on the Cloudflare Workers platform, but could theoretically be exploitable on deployments of workerd running on machines with a huge amount of memory. Moreover, in order to be remotely exploited, an attacker would have to upload a single form-encoded HTTP request of at least tens of gigabytes in size. The application code would then have to use request.formData() to parse the request and formData.forEach() to iterate over this data. Due to these limitations, the exploitation likelihood was considered Low. A fix that addresses this vulnerability has been released in version v1.20230419.0 and users are encouraged to update to the latest version available.	6.5	More Details
CVE-2023-31555	podofoinfo 0.10.0 was discovered to contain a segmentation violation via the function PoDoFo::PdfObject::DelayedLoad.	6.5	More Details
CVE-2023-31556	podofoinfo 0.10.0 was discovered to contain a segmentation violation via the function PoDoFo::PdfDictionary::findKeyParent.	6.5	More Details
CVE-2023-32990	A missing permission check in Jenkins Azure VM Agents Plugin 852.v8d35f0960a_43 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified Azure Cloud server using attacker-specified credentials IDs obtained through another method.	6.5	More Details
CVE-2023-28325	An improper authorization vulnerability exists in Rocket.Chat <6.0 that could allow a hacker to manipulate the rid parameter and change the updateMessage method that only checks whether the user is allowed to edit message in the target room.	6.5	More Details
CVE-2023-27562	The n8n package 0.218.0 for Node.js allows Directory Traversal.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2088	A flaw was found in OpenStack due to an inconsistency between Cinder and Nova. This issue can be triggered intentionally or by accident. A remote, authenticated attacker could exploit this vulnerability by detaching one of their volumes from Cinder. The highest impact is to confidentiality.	6.5	More Details
CVE-2023-2179	The WooCommerce Order Status Change Notifier WordPress plugin through 1.1.0 does not have authorisation and CSRF when updating status orders via an AJAX action available to any authenticated users, which could allow low privilege users such as subscriber to update arbitrary order status, making them paid without actually paying for them for example	6.5	More Details
CVE-2023-32081	Vert.x STOMP is a vert.x implementation of the STOMP specification that provides a STOMP server and client. From versions 3.1.0 until 3.9.16 and 4.0.0 until 4.4.2, a Vert.x STOMP server processes client STOMP frames without checking that the client send an initial CONNECT frame replied with a successful CONNECTED frame. The client can subscribe to a destination or publish message without prior authentication. Any Vert.x STOMP server configured with an authentication handler is impacted. The issue is patched in Vert.x 3.9.16 and 4.4.2. There are no trivial workarounds.	6.5	More Details
CVE-2023-23867	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Gautam Thapar Button Builder – Buttons X plugin <= 0.8.6 versions.	6.5	More Details
CVE-2023-23873	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Flector BBSpoiler plugin <= 2.01 versions.	6.5	More Details
CVE-2023-22696	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Custom4Web Affiliate Links Lite plugin <= 2.5 versions.	6.5	More Details
CVE-2022-46377	An out-of-bounds read vulnerability exists in the PORT command parameter extraction functionality of Weston Embedded uC-FTPs v 1.98.00. A specially-crafted set of network packets can lead to denial of service. An attacker can send packets to trigger this vulnerability.This vulnerability occurs when no IP address argument is provided to the `PORT` command.	6.5	More Details
CVE-2023-23703	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Tyche Softwares Arconix Shortcodes plugin <= 2.1.7 versions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22711	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Agent Evolution IMPress Listings plugin <= 2.6.2 versions.	6.5	More Details
CVE-2023-23657	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Richard Leishman t/a Webforward Mail Subscribe List plugin <= 2.1.9 versions.	6.5	More Details
CVE-2023-23641	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WPmanage Uji Popup plugin <= 1.4.3 versions.	6.5	More Details
CVE-2023-23676	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Bruno "Aesqe" Babic File Gallery plugin <= 1.8.5.3 versions.	6.5	More Details
CVE-2022-47378	Multiple CODESYS products in multiple versions are prone to a improper input validation vulnerability. An authenticated remote attacker may craft specific requests that use the vulnerability leading to a denial-of-service condition.	6.5	More Details
CVE-2023-25070	Cleartext transmission of sensitive information exists in SkyBridge MB-A100/110 firmware Ver. 4.2.0 and earlier. If the telnet connection is enabled, a remote unauthenticated attacker may eavesdrop on or alter the administrator's communication to the product.	6.5	More Details
CVE-2023-24586	Cleartext storage of sensitive information exists in SkyBridge MB-A100/110 firmware Ver. 4.2.0 and earlier, which may allow a remote authenticated attacker to obtain an APN credential for the product.	6.5	More Details
CVE-2022-40685	Insufficiently protected credentials in the Intel(R) DCM software before version 5.0.1 may allow an authenticated user to potentially enable information disclosure via network access.	6.5	More Details
CVE-2023-23901	Improper following of a certificate's chain of trust exists in SkyBridge MB-A200 firmware Ver. 01.00.05 and earlier, and SkyBridge BASIC MB-A130 firmware Ver. 1.4.1 and earlier, which may allow a remote unauthenticated attacker to eavesdrop on or alter the communication sent to the WebUI of the product.	6.5	More Details
CVE-2023-22717	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in nCrafts FormCraft plugin <= 1.2.6 versions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22361	Improper privilege management vulnerability in SkyBridge MB-A100/110 firmware Ver. 4.2.0 and earlier allows a remote authenticated attacker to alter a WebUI password of the product.	6.5	More Details
CVE-2023-25927	IBM Security Verify Access 10.0.0, 10.0.1, 10.0.2, 10.0.3, 10.0.4, and 10.0.5 could allow an attacker to crash the webseald process using specially crafted HTTP requests resulting in loss of access to the system. IBM X-Force ID: 247635.	6.5	More Details
CVE-2022-47393	An authenticated, remote attacker may use a Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in multiple versions of multiple CODESYS products to force a denial-of-service situation.	6.5	More Details
CVE-2022-47392	An authenticated, remote attacker may use a improper input validation vulnerability in the CmpApp/CmpAppBP/CmpAppForce Components of multiple CODESYS products in multiple versions to read from an invalid address which can lead to a denial-of-service condition.	6.5	More Details
CVE-2023-23169	Synapsoft pdfocus 1.17 is vulnerable to local file inclusion and server-side request forgery Directory Traversal.	6.5	More Details
CVE-2023-23701	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Andrew @ Geeenville Web Design Easy Sign Up plugin <= 3.4.1 versions.	6.5	More Details
CVE-2023-23709	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Denis WPJAM Basic plugin <= 6.2.1 versions.	6.5	More Details
CVE-2023-28361	A Cross-site WebSocket Hijacking (CSWSH) vulnerability found in UniFi OS 2.5 and earlier allows a malicious actor to access certain confidential information by persuading a UniFi OS user to visit a malicious webpage.Affected Products:Cloud Key Gen2Cloud Key Gen2 PlusUNVRUNVR ProfessionalUDMUDM ProfessionalUDM SEUDRMitigation:Update affected products to UniFi OS 3.0.13 or later.	6.5	More Details
CVE-2023-32573	In Qt before 5.15.14, 6.0.x through 6.2.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.1, QtSvg QSvgFont m_unitsPerEm initialization is mishandled.	6.5	More Details
CVE-2022-41771	Incorrect permission assignment for critical resource in some Intel(R) QAT drivers for Windows before version 1.9.0 may allow an authenticated user to potentially enable information disclosure via local access.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30281	Insecure permissions vulnerability was discovered, due to a lack of permissions's control in scquickaccounting before v3.7.3 from Store Commander for PrestaShop, a guest can access exports from the module which can lead to leak of personnal informations from ps_customer table sush as name / surname / email	6.5	More Details
CVE-2023-1729	A flaw was found in LibRaw. A heap-buffer-overflow in raw2image_ex() caused by a maliciously crafted file may lead to an application crash.	6.5	More Details
CVE-2023-22720	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Robert Macchi WP Links Page plugin <= 4.9.3 versions.	6.5	More Details
CVE-2023-28520	IBM Planning Analytics Local 2.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 250454.	6.4	More Details
CVE-2023-2690	A vulnerability, which was classified as critical, has been found in SourceCodester Personnel Property Equipment System 1.0. This issue affects some unknown processing of the file admin/returned_reuse_form.php of the component GET Parameter Handler. The manipulation of the argument client_id 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-228971.	6.3	More Details
CVE-2023-2656	A vulnerability classified as critical has been found in SourceCodester AC Repair and Services System 1.0. Affected is an unknown function of the file /classes/Master.php?f=delete_service. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-228798 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2642	A vulnerability classified as critical has been found in SourceCodester Online Exam System 1.0. This affects an unknown part of the file adminpanel/admin/facebox_modal/updateCourse.php of the component GET Parameter Handler. 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-228771.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25776	Improper input validation in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable information disclosure via local access.	6.3	More Details
CVE-2023-2659	A vulnerability, which was classified as critical, was found in SourceCodester Online Computer and Laptop Store 1.0. This affects an unknown part of the file view_product.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-228801 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2698	A vulnerability classified as critical was found in SourceCodester Lost and Found Information System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/?page=items/manage_item of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-228979.	6.3	More Details
CVE-2023-2660	A vulnerability has been found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. This vulnerability affects unknown code of the file view_categories.php. The manipulation of the argument c leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-228802 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-28411	Double free in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable information disclosure via local access.	6.3	More Details
CVE-2023-2697	A vulnerability classified as critical has been found in SourceCodester Online Exam System 1.0. Affected is an unknown function of the file /jurusan/data of the component POST Parameter Handler. The manipulation of the argument columns[1][data] leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-228978 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-27554	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 249185.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2643	A vulnerability classified as critical was found in SourceCodester File Tracker Manager System 1.0. This vulnerability affects unknown code of the file register/update_password.php of the component POST Parameter Handler. The manipulation of the argument new_password leads to sql injection. 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-228772.	6.3	More Details
CVE-2023-2695	A vulnerability was found in SourceCodester Online Exam System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /kelas/data of the component POST Parameter Handler. The manipulation of the argument columns[1][data] leads to sql injection. 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-228976.	6.3	More Details
CVE-2023-2653	A vulnerability classified as critical was found in SourceCodester Lost and Found Information System 1.0. Affected by this vulnerability is an unknown functionality of the file items/index.php. The manipulation of the argument cid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-228781 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2661	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. This issue affects some unknown processing of the file /classes/Master.php. The manipulation of the argument id 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-228803.	6.3	More Details
CVE-2023-2652	A vulnerability classified as critical has been found in SourceCodester Lost and Found Information System 1.0. Affected is an unknown function of the file /classes/Master.php?f=delete_item. The manipulation 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-228780.	6.3	More Details
CVE-2023-2696	A vulnerability was found in SourceCodester Online Exam System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /matkul/data of the component POST Parameter Handler. The manipulation of the argument columns[1][data] 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-228977 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2647	A vulnerability was found in Weaver E-Office 9.5 and classified as critical. Affected by this issue is some unknown functionality of the file /webroot/inc/utility_all.php of the component File Upload Handler. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-228776. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-2738	A vulnerability classified as critical has been found in Tongda OA 11.10. This affects the function actionGetdata of the file GatewayController.php. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-229149 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2022-29508	Null pointer dereference in the Intel(R) VROC software before version 7.7.6.1003 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.3	More Details
CVE-2023-2670	A vulnerability was found in SourceCodester Lost and Found Information System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file admin/?page=user/manage_user. The manipulation leads to improper access controls. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-228886 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2668	A vulnerability was found in SourceCodester Lost and Found Information System 1.0 and classified as critical. Affected by this issue is the function manager_category of the file admin/?page=categories/manage_category of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-228884.	6.3	More Details
CVE-2023-2689	A vulnerability classified as critical was found in SourceCodester Billing Management System 1.0. This vulnerability affects unknown code of the file editproduct.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-228970 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2181	An issue has been discovered in GitLab affecting all versions before 15.9.8, 15.10.0 before 15.10.7, and 15.11.0 before 15.11.3. A malicious developer could use a git feature called refs/replace to smuggle content into a merge request which would not be visible during review in the UI.	6.3	More Details
CVE-2023-2677	A vulnerability, which was classified as critical, was found in SourceCodester Covid-19 Contact Tracing System 1.0. This affects an unknown part of the file admin/establishment/manage.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-228891.	6.3	More Details
CVE-2023-2672	A vulnerability classified as critical has been found in SourceCodester Lost and Found Information System 1.0. Affected is an unknown function of the file items/view.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-228888.	6.3	More Details
CVE-2023-2619	A vulnerability, which was classified as critical, was found in SourceCodester Online Tours & Travels Management System 1.0. This affects the function exec of the file disapprove_delete.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-228549 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2669	A vulnerability was found in SourceCodester Lost and Found Information System 1.0. It has been classified as critical. This affects an unknown part of the file admin/?page=categories/view_category of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-228885 was assigned to this vulnerability.	6.3	More Details
CVE-2023-2648	A vulnerability was found in Weaver E-Office 9.5. It has been classified as critical. This affects an unknown part of the file /inc/jquery/uploadify/uploadify.php. The manipulation of the argument Filedata leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-228777 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2682	A vulnerability was found in Caton Live up to 2023-04-26 and classified as critical. This issue affects some unknown processing of the file /cgi-bin/ping.cgi of the component Mini_HTTPD. The manipulation of the argument address with the input ;id;uname${IFS}-a leads to command injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-228911. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-2658	A vulnerability, which was classified as critical, has been found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this issue is some unknown functionality of the file products.php. The manipulation of the argument c leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-228800.	6.3	More Details
CVE-2023-2694	A vulnerability was found in SourceCodester Online Exam System 1.0. It has been classified as critical. This affects an unknown part of the file /dosen/data of the component POST Parameter Handler. The manipulation of the argument columns[1][data] 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-228975.	6.3	More Details
CVE-2023-2693	A vulnerability was found in SourceCodester Online Exam System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /mahasiswa/data of the component POST Parameter Handler. The manipulation of the argument columns[1][data] leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-228974 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-2699	A vulnerability, which was classified as critical, has been found in SourceCodester Lost and Found Information System 1.0. Affected by this issue is some unknown functionality of the file admin/?page=items/view_item of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-228980.	6.3	More Details
CVE-2023-23450	Use of Password Hash Instead of Password for Authentication in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows an unprivileged remote attacker to use a password hash instead of an actual password to login to a valid user account via the REST interface.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2708	The Video Gallery plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘search_term’ parameter in versions up to, and including, 1.0.10 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-28358	A vulnerability has been discovered in Rocket.Chat where a markdown parsing issue in the "Search Messages" feature allows the insertion of malicious tags. This can be exploited on servers with content security policy disabled possible leading to some issues attacks like account takeover.	6.1	More Details
CVE-2023-27237	LavaLite CMS v 9.0.0 was discovered to be vulnerable to a host header injection attack.	6.1	More Details
CVE-2022-37327	Improper input validation in BIOS firmware for Intel(R) NUC, Intel(R) NUC Performance Kit, Intel(R) NUC Performance Mini PC, Intel(R) NUC 8 Compute Element, Intel(R) NUC Pro Kit, Intel(R) NUC Pro Board, Intel(R) NUC 11 Compute Element, Intel(R) NUC 12 Compute Element, Intel(R) NUC Extreme, Intel(R) NUC 12 Extreme Compute Element, Intel(R) NUC Laptop Kit, Intel(R) NUC Enthusiast, Intel(R) NUC Essential, Intel(R) NUC Laptop Kit, Intel(R) NUC Extreme Compute Element, Intel(R) NUC Boards, Intel(R) NUC Pro Compute Element, Intel(R) NUC Rugged may allow a privileged user to enable information disclosure via local access.	6.1	More Details
CVE-2023-30256	Cross Site Scripting vulnerability found in Webkil QloApps v.1.5.2 allows a remote attacker to obtain sensitive information via the back and email_create parameters in the AuthController.php file.	6.1	More Details
CVE-2023-25309	Cross Site Scripting (XSS) Vulnerability in Fetlife rollout-ui version 0.5, allows attackers to execute arbitrary code via a crafted url to the delete a feature functionality.	6.1	More Details
CVE-2023-29791	kodbox <= 1.37 is vulnerable to Cross Site Scripting (XSS) via the debug information.	6.1	More Details
CVE-2023-2710	The video carousel slider with lightbox plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search_term parameter in versions up to, and including, 1.0.22 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27918	Cross-site scripting vulnerability in Appointment and Event Booking Calendar for WordPress - Amelia versions prior to 1.0.76 allows a remote unauthenticated attacker to inject an arbitrary script by having a user who is logging in the WordPress where the product is installed visit a malicious URL.	6.1	More Details
CVE-2023-25175	Improper input validation in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable information disclosure via local access.	6.1	More Details
CVE-2023-30394	The MoveIt framework 1.1.11 for ROS allows cross-site scripting (XSS) via the API authentication function.	6.1	More Details
CVE-2022-48020	Vinteo VCC v2.36.4 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the conference parameter. This vulnerability allows attackers to inject arbitrary code which will be executed by the victim user's browser.	6.1	More Details
CVE-2023-1596	The tagDiv Composer WordPress plugin before 4.0 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-1835	The Ninja Forms Contact Form WordPress plugin before 3.6.22 does not properly escape user input before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2021-39036	IBM Cognos Analytics 11.1 and 11.2 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: 213966.	6.1	More Details
CVE-2023-1890	The Tablesome WordPress plugin before 1.0.9 does not escape various generated URLs, before outputting them in attributes when some notices are displayed, leading to Reflected Cross-Site Scripting	6.1	More Details
CVE-2023-1915	The Thumbnail carousel slider WordPress plugin before 1.1.10 does not sanitise and escape some parameters before outputting them back in pages, leading to Reflected Cross-Site Scripting vulnerability which could be used against high privilege users such as admin.	6.1	More Details
CVE-2023-29808	Cross Site Scripting (XSS) vulnerability in vogtmh cmaps (companymaps) 8.0 allows attackers to execute arbitrary code.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0644	The Push Notifications for WordPress by PushAssist WordPress plugin through 3.0.8 does not sanitise and escape various parameters before outputting them back in pages, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	6.1	More Details
CVE-2023-24475	Out of bounds read in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable information disclosure via local access.	6.0	More Details
CVE-2023-22443	Integer overflow in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable denial of service via local access.	6.0	More Details
CVE-2022-43475	Insecure storage of sensitive information in the Intel(R) DCM software before version 5.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.0	More Details
CVE-2023-27870	IBM Spectrum Virtualize 8.5, under certain circumstances, could disclose sensitive credential information while a download from Fix Central is in progress. IBM X-Force ID: 249518.	5.9	More Details
CVE-2022-47606	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Tim Stephenson WP-CORS plugin <= 0.2.1 versions.	5.9	More Details
CVE-2022-47587	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Cornel Raiu WP Search Analytics plugin <= 1.4.5 versions.	5.9	More Details
CVE-2022-47436	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MantraBrain Yatra allows Stored XSS.This issue affects Yatra: from n/a through 2.1.14.	5.9	More Details
CVE-2022-46817	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Flyzoo Flyzoo Chat plugin <= 2.3.3 versions.	5.9	More Details
CVE-2023-23682	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Snap Creek Software EZP Maintenance Mode plugin <= 1.0.1 versions.	5.9	More Details
CVE-2023-23683	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Ozan Canakli White Label Branding for Elementor Page Builder plugin <= 1.0.2 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47423	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Ulf Benjaminsson WP-dTree plugin <= 4.4.5 versions.	5.9	More Details
CVE-2022-46819	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Continuous announcement scroller plugin <= 13.0 versions.	5.9	More Details
CVE-2023-28076	CloudLink 7.1.2 and all prior versions contain a broken or risky cryptographic algorithm vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability leading to some information disclosure.	5.9	More Details
CVE-2023-30746	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Booqable Rental Software Booqable Rental plugin <= 2.4.15 versions.	5.9	More Details
CVE-2023-23654	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in SparkPost plugin <= 3.2.5 versions.	5.9	More Details
CVE-2023-28414	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in ApexChat plugin <= 1.3.1 versions.	5.9	More Details
CVE-2023-24406	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Muneeb ur Rehman Simple PopUp plugin <= 1.8.6 versions.	5.9	More Details
CVE-2023-23794	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alex Moss Semalt Blocker plugin <= 1.1.3 versions.	5.9	More Details
CVE-2023-22684	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Subscribers.Com Subscribers plugin <= 1.5.3 versions.	5.9	More Details
CVE-2023-28932	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPMobile.App WPMobile.App — Android and iOS Mobile Application plugin <= 11.20 versions.	5.9	More Details
CVE-2023-24418	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Tiny carousel horizontal slider plus plugin <= 3.2 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23812	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Joost de Valk Enhanced WP Contact Form plugin <= 2.2.3 versions.	5.9	More Details
CVE-2023-23789	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Premmerce Premmerce Redirect Manager plugin <= 1.0.9 versions.	5.9	More Details
CVE-2023-25958	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Justin Saad Simple Tooltips plugin <= 2.1.4 versions.	5.9	More Details
CVE-2023-23788	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Florin Arjocu Custom More Link Complete plugin <= 1.4.1 versions.	5.9	More Details
CVE-2023-31161	An Improper Input Validation vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow an authenticated remote attacker to use internal resources, allowing a variety of potential effects. See SEL Service Bulletin dated 2022-11-15 for more details.	5.9	More Details
CVE-2023-23786	Auth. (editor+) Stored Cross-Site Scripting (XSS) vulnerability in Christof Servit affiliate-toolkit plugin <= 3.3.3 versions.	5.9	More Details
CVE-2023-25460	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in CodeSolz Easy Ad Manager plugin <= 1.0.0 versions.	5.9	More Details
CVE-2023-22690	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Shopfiles Ltd Ebook Store plugin <= 5.775 versions.	5.9	More Details
CVE-2023-32570	VideoLAN dav1d before 1.2.0 has a thread_task.c race condition that can lead to an application crash, related to dav1d_decode_frame_exit.	5.9	More Details
CVE-2023-23810	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in SnapOrbital Panorama plugin <= 1.5 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0857	Unintentional change of settings during initial registration of system administrators which uses control protocols. The affected Office / Small Office Multifunction Printers and Laser Printers(*) may allow an attacker on the network segment to trigger unauthorized access to the product. *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe.	5.9	More Details
CVE-2023-23674	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in RVOLA WP Original Media Path plugin <= 2.4.0 versions.	5.9	More Details
CVE-2023-23673	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Harish Chouhan, Themeist I Recommend This plugin <= 3.8.3 versions.	5.9	More Details
CVE-2022-47137	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPManageNinja LLC Ninja Tables plugin <= 4.3.4 versions.	5.9	More Details
CVE-2023-23727	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Formilla Live Chat by Formilla plugin <= 1.3 versions.	5.9	More Details
CVE-2022-46861	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Zia Imtiaz Custom Login Page Styler for WordPress plugin <= 6.2 versions.	5.9	More Details
CVE-2023-23720	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in NetReviews SAS Verified Reviews (Avis Vérifiés) plugin <= 2.3.13 versions.	5.9	More Details
CVE-2023-22685	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Tips and Tricks HQ, Ruhul Amin Category Specific RSS feed Subscription plugin <= v2.2 versions.	5.9	More Details
CVE-2023-2490	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Fernando Briano UserAgent-Spy plugin <= 1.3.1 versions.	5.9	More Details
CVE-2023-25771	Improper access control for some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable denial of service via local access.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38787	Improper input validation in firmware for some Intel(R) FPGA products before version 2.7.0 Hotfix may allow an authenticated user to potentially enable escalation of privilege via local access.	5.7	More Details
CVE-2022-21239	Out-of-bounds read in software for the Intel QAT Driver for Windows before version 1.9.0-0008 may allow an authenticated user to potentially enable information disclosure via local access.	5.6	More Details
CVE-2023-31919	Jerryscript 3.0 (commit 05dbbd1) was discovered to contain an Assertion Failure via the jcontext_raise_exception at jerry-core/jcontext/jcontext.c.	5.5	More Details
CVE-2023-31920	Jerryscript 3.0 (commit 05dbbd1) was discovered to contain an Assertion Failure via the vm_loop at jerry-core/vm/vm.c.	5.5	More Details
CVE-2023-2676	A vulnerability, which was classified as critical, has been found in H3C R160 V1004004. Affected by this issue is some unknown functionality of the file /goForm/aspForm. The manipulation of the argument go leads to stack-based buffer overflow. The exploit has been disclosed to the public and may be used. VDB-228890 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-29286	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-32668	LuaTeX before 1.17.0 allows a document (compiled with the default settings) to make arbitrary network requests. This occurs because full access to the socket library is permitted by default, as stated in the documentation. This also affects TeX Live before 2023 r66984 and MiKTeX before 23.5.	5.5	More Details
CVE-2023-31918	Jerryscript 3.0 (commit 1a2c047) was discovered to contain an Assertion Failure via the parser_parse_function_arguments at jerry-core/parser/js/js-parser.c.	5.5	More Details
CVE-2023-31913	Jerryscript 3.0 *commit 1a2c047) was discovered to contain an Assertion Failure via the component parser_parse_class at jerry-core/parser/js/js-parser-expr.c.	5.5	More Details
CVE-2023-31916	Jerryscript 3.0 (commit 1a2c047) was discovered to contain an Assertion Failure via the jmem_heap_finalize at jerry-core/jmem/jmem-heap.c.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31914	Jerryscript 3.0 (commit 05dbbd1) was discovered to contain out-of-memory issue in malloc.	5.5	More Details
CVE-2023-29818	An issue found in Webroot SecureAnywhere Endpoint Protection CE 23.1 v.9.0.33.39 and before allows a local attacker to bypass protections via the default allowlist feature being stored as non-admin.	5.5	More Details
CVE-2023-29819	An issue found in Webroot SecureAnywhere Endpoint Protection CE 23.1 v.9.0.33.39 and before allows a local attacker to bypass protections via a crafted payload.	5.5	More Details
CVE-2023-29820	An issue found in Webroot SecureAnywhere Endpoint Protection CE 23.1 v.9.0.33.39 and before allows a local attacker to access sensitive information via the EXE installer. NOTE: the vendor's perspective is that this is not a separate vulnerability relative to CVE-2023-29818 and CVE-2023-29819.	5.5	More Details
CVE-2023-29024	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product A cross site scripting vulnerability was discovered that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.	5.5	More Details
CVE-2023-20914	In onSetRuntimePermissionGrantStateByDeviceAdmin of AdminRestrictedPermissionsUtils.java, there is a possible way for the work profile to read SMS messages due to a permissions bypass. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-189942529	5.5	More Details
CVE-2023-31921	Jerryscript 3.0 (commit 05dbbd1) was discovered to contain an Assertion Failure via the ecma_big_uint_div_mod at jerry-core/ecma/operations/ecma-big-uint.c.	5.5	More Details
CVE-2023-21112	In AnalyzeMfcResp of NxpMfcReader.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-252763983	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20930	In pushDynamicShortcut of ShortcutPackage.java, there is a possible way to get the device into a boot loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-250576066	5.5	More Details
CVE-2023-21103	In registerPhoneAccount of PhoneAccountRegistrar.java, uncaught exceptions in parsing persisted user data could lead to local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-259064622	5.5	More Details
CVE-2023-21104	In applySyncTransaction of WindowOrganizer.java, a missing permission check could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12L Android-13Android ID: A-259938771	5.5	More Details
CVE-2023-32076	in-toto is a framework to protect supply chain integrity. The in-toto configuration is read from various directories and allows users to configure the behavior of the framework. The files are from directories following the XDG base directory specification. In versions 1.4.0 and prior, among the files read is `.in_totorc` which is a hidden file in the directory in which in-toto is run. If an attacker controls the inputs to a supply chain step, they can mask their activities by also passing in an `.in_totorc` file that includes the necessary exclude patterns and settings. RC files are widely used in other systems and security issues have been discovered in their implementations as well. Maintainers found in their conversations with in-toto adopters that `in_totorc` is not their preferred way to configure in-toto. As none of the options supported in `in_totorc` is unique, and can be set elsewhere using API parameters or CLI arguments, the maintainers decided to drop support for `in_totorc`. in-toto's `user_settings` module has been dropped altogether in commit 3a21d84f40811b7d191fa7bd17265c1f99599afd. Users may also sandbox functionary code as a security measure.	5.5	More Details
CVE-2023-29277	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-4008	In affected versions of Octopus Deploy it is possible to upload a zipbomb file as a task which results in Denial of Service	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21111	In several functions of PhoneAccountRegistrar.java, there is a possible way to prevent an access to emergency services due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-256819769	5.5	More Details
CVE-2023-20706	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767860; Issue ID: ALPS07767860.	5.5	More Details
CVE-2023-20705	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767870; Issue ID: ALPS07767870.	5.5	More Details
CVE-2023-20704	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767826; Issue ID: ALPS07767826.	5.5	More Details
CVE-2023-20703	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767853; Issue ID: ALPS07767853.	5.5	More Details
CVE-2023-21118	In unflattenString8 of Sensor.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-269014004	5.5	More Details
CVE-2022-25976	Improper input validation in the Intel(R) VROC software before version 7.7.6.1003 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2023-29279	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2700	A vulnerability was found in libvirt. This security flaw ouccers due to repeatedly querying an SR-IOV PCI device's capabilities that exposes a memory leak caused by a failure to free the virPCIVirtualFunction array within the parent struct's g_autoptr cleanup.	5.5	More Details
CVE-2023-2616	Cross-site Scripting (XSS) - Generic in GitHub repository pimcore/pimcore prior to 10.5.21.	5.4	More Details
CVE-2022-41979	Protection mechanism failure in the Intel(R) DCM software before version 5.1 may allow an authenticated user to potentially enable escalation of privilege via network access.	5.4	More Details
CVE-2023-27888	Cross-site scripting vulnerability in Joruri Gw Ver 3.2.5 and earlier allows a remote authenticated attacker to inject an arbitrary script via Message Memo function of the affected product.	5.4	More Details
CVE-2023-29983	Cross Site Scripting vulnerability found in Maximilian Vogt cmaps v.8.0 allows a remote attacker to execute arbitrary code via the auditlog tab in the admin panel.	5.4	More Details
CVE-2022-44610	Improper authentication in the Intel(R) DCM software before version 5.1 may allow an authenticated user to potentially enable escalation of privilege via network access.	5.4	More Details
CVE-2023-2614	Cross-site Scripting (XSS) - DOM in GitHub repository pimcore/pimcore prior to 10.5.21.	5.4	More Details
CVE-2023-2615	Cross-site Scripting (XSS) - Reflected in GitHub repository pimcore/pimcore prior to 10.5.21.	5.4	More Details
CVE-2021-27131	Moodle 3.10.1 is vulnerable to persistent/stored cross-site scripting (XSS) due to the improper input sanitization on the "Additional HTML Section" via "Header and Footer" parameter in /admin/settings.php. This vulnerability is leading an attacker to steal admin and all user account cookies by storing the malicious XSS payload in Header and Footer. NOTE: this is disputed by the vendor because the "Additional HTML Section" for "Header and Footer" can only be supplied by an administrator, who is intentionally allowed to enter unsanitized input (e.g., site-specific JavaScript).	5.4	More Details
CVE-2023-33007	Jenkins LoadComplete support Plugin 1.0 and earlier does not escape the LoadComplete test name, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33006	A cross-site request forgery (CSRF) vulnerability in Jenkins WSO2 Oauth Plugin 1.0 and earlier allows attackers to trick users into logging in to the attacker's account.	5.4	More Details
CVE-2023-33005	Jenkins WSO2 Oauth Plugin 1.0 and earlier does not invalidate the previous session on login.	5.4	More Details
CVE-2023-33002	Jenkins TestComplete support Plugin 2.8.1 and earlier does not escape the TestComplete project name, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2023-1019	The Help Desk WP WordPress plugin through 1.2.0 does not sanitise and escape some parameters, which could allow users with a role as low as Editor to perform Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-31544	A stored cross-site scripting (XSS) vulnerability in alkacon-OpenCMS v11.0.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Title field under the Upload Image module.	5.4	More Details
CVE-2023-32984	Jenkins TestNG Results Plugin 730.v4c5283037693 and earlier does not escape several values that are parsed from TestNG report files and displayed on the plugin's test information pages, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide a crafted TestNG report file.	5.4	More Details
CVE-2023-0520	The RapidExpCart WordPress plugin through 1.0 does not sanitize and escape the url parameter in the rapidexpcart endpoint before storing it and outputting it back in the page, leading to a Stored Cross-Site Scripting vulnerability which could be used against high-privilege users such as admin, furthermore lack of csrf protection means an attacker can trick a logged in admin to perform the attack by submitting a hidden form.	5.4	More Details
CVE-2023-0490	The f(x) TOC WordPress plugin through 1.1.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-32977	Jenkins Pipeline: Job Plugin does not escape the display name of the build that caused an earlier build to be aborted, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to set build display names immediately.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2730	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.3.3.	5.4	More Details
CVE-2023-25833	There is an HTML injection vulnerability in Esri Portal for ArcGIS versions 11.0 and below that may allow a remote, authenticated attacker to create a crafted link which when clicked could render arbitrary HTML in the victim's browser (no stateful change made or customer data rendered).	5.4	More Details
CVE-2022-45846	Cross-Site Request Forgery (CSRF) vulnerability in Nickys Image Map Pro for WordPress - Interactive SVG Image Map Builder plugin < 5.6.9 versions.	5.4	More Details
CVE-2023-0233	The ActiveCampaign WordPress plugin before 8.1.12 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-32582	Improper access control in firmware for some Intel(R) NUC Boards, Intel(R) NUC 11 Performance Kit, Intel(R) NUC 11 Performance Mini PC, Intel(R) NUC Pro Compute Element may allow a privileged user to potentially enable denial of service via local access.	5.3	More Details
CVE-2023-31678	Incorrect access control in Videogo v6.8.1 allows attackers to bind shared devices after the connection has been ended.	5.3	More Details
CVE-2023-28936	Attacker can access arbitrary recording/room Vendor: The Apache Software Foundation Versions Affected: Apache OpenMeetings from 2.0.0 before 7.1.0	5.3	More Details
CVE-2023-29986	spring-boot-actuator-logview 0.2.13 allows Directory Traversal to sibling directories via LogViewEndpoint.view.	5.3	More Details
CVE-2023-27919	Authentication bypass vulnerability in NEXT ENGINE Integration Plugin (for EC-CUBE 2.0 series) all versions allows a remote unauthenticated attacker to alter the information stored in the system.	5.3	More Details
CVE-2023-28359	A NoSQL injection vulnerability has been identified in the listEmojiCustom method call within Rocket.Chat. This can be exploited by unauthenticated users when there is at least one custom emoji uploaded to the Rocket.Chat instance. The vulnerability causes a delay in the server response, with the potential for limited impact.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2644	A vulnerability, which was classified as problematic, has been found in DigitalPersona FPSensor 1.0.0.1. This issue affects some unknown processing of the file C:\Program Files (x86)\FPSensor\bin\DpHost.exe. The manipulation leads to unquoted search path. Attacking locally is a requirement. The identifier VDB-228773 was assigned to this vulnerability.	5.3	More Details
CVE-2023-32313	vm2 is a sandbox that can run untrusted code with Node's built-in modules. In versions 3.9.17 and lower of vm2 it was possible to get a read-write reference to the node `inspect` method and edit options for `console.log`. As a result a threat actor can edit options for the `console.log` command. This vulnerability was patched in the release of version `3.9.18` of `vm2`. Users are advised to upgrade. Users unable to upgrade may make the `inspect` method readonly with `vm.readonly(inspect)` after creating a vm.	5.3	More Details
CVE-2023-31409	Uncontrolled Resource Consumption in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows an remote attacker to influence the availability of the webserver by invocing a Slowloris style attack via HTTP requests.	5.3	More Details
CVE-2023-31445	Cassia Access controller before 2.1.1.2203171453, was discovered to have a unprivileged -information disclosure vulnerability that allows read-only users have the ability to enumerate all other users and discover e-mail addresses, phone numbers, and privileges of all other users.	5.3	More Details
CVE-2023-31408	Cleartext Storage of Sensitive Information in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows a remote attacker to potentially steal user credentials that are stored in the user’s browsers local storage via cross-site-scripting attacks.	5.3	More Details
CVE-2023-23449	Observable Response Discrepancy in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows a remote attacker to gain information about valid usernames by analyzing challenge responses from the server via the REST interface.	5.3	More Details
CVE-2023-23448	Inclusion of Sensitive Information in Source Code in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows a remote attacker to gain information about valid usernames via analysis of source code.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2617	A vulnerability classified as problematic was found in OpenCV wechat_qrcode Module up to 4.7.0. Affected by this vulnerability is the function DecodedBitStreamParser::decodeByteSegment of the file qrcode/decoder/decoded_bit_stream_parser.cpp. The manipulation leads to null pointer dereference. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-228547.	5.3	More Details
CVE-2023-2618	A vulnerability, which was classified as problematic, has been found in OpenCV wechat_qrcode Module up to 4.7.0. Affected by this issue is the function DecodedBitStreamParser::decodeHanziSegment of the file qrcode/decoder/decoded_bit_stream_parser.cpp. The manipulation leads to memory leak. The attack may be launched remotely. The name of the patch is 2b62ff6181163eea029ed1cab11363b4996e9cd6. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-228548.	5.3	More Details
CVE-2023-1732	When sampling randomness for a shared secret, the implementation of Kyber and FrodoKEM, did not check whether crypto/rand.Read() returns an error. In rare deployment cases (error thrown by the Read() function), this could lead to a predictable shared secret. The tkn20 and blindrsa components did not check whether enough randomness was returned from the user provided randomness source. Typically the user provides crypto/rand.Reader, which in the vast majority of cases will always return the right number random bytes. In the cases where it does not, or the user provides a source that does not, the blinding for blindrsa is weak and integrity of the plaintext is not ensured in tkn20.	5.3	More Details
CVE-2022-47880	An Information disclosure vulnerability in /be/rpc.php in Jedox GmbH Jedox 2020.2.5 allow remote, authenticated users with permissions to modify database connections to disclose a connections' cleartext password via the 'test connection' function.	5.3	More Details
CVE-2023-32983	Jenkins Ansible Plugin 204.v8191fd551eb_f and earlier does not mask extra variables displayed on the configuration form, increasing the potential for attackers to observe and capture them.	5.3	More Details
CVE-2023-32303	Planet is software that provides satellite data. The secret file stores the user's Planet API authentication information. It should only be accessible by the user, but before version 2.0.1, its permissions allowed the user's group and non-group to read the file as well. This issue was patched in version 2.0.1. As a workaround, set the secret file permissions to only user read/write by hand.	5.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29840	Server-Side Request Forgery (SSRF) vulnerability that could allow a rogue server on the local network to modify its URL to point back to the loopback adapter was addressed in Western Digital My Cloud OS 5 devices. This could allow the URL to exploit other vulnerabilities on the local server.This issue affects My Cloud OS 5 devices before 5.26.202.	5.1	More Details
CVE-2022-41801	Uncontrolled resource consumption in the Intel(R) Connect M Android application before version 1.82 may allow an authenticated user to potentially enable denial of service via local access.	5.0	More Details
CVE-2023-2161	A CWE-611: Improper Restriction of XML External Entity Reference vulnerability exists that could cause unauthorized read access to the file system when a malicious configuration file is loaded on to the software by a local user.	5.0	More Details
CVE-2023-25179	Uncontrolled resource consumption in the Intel(R) Unite(R) android application before Release 17 may allow an authenticated user to potentially enable denial of service via local access.	5.0	More Details
CVE-2022-41610	Improper authorization in Intel(R) EMA Configuration Tool before version 1.0.4 and Intel(R) MC before version 2.4 software may allow an authenticated user to potentially enable denial of service via local access.	5.0	More Details
CVE-2022-46645	Uncontrolled resource consumption in the Intel(R) Smart Campus Android application before version 9.9 may allow an authenticated user to potentially enable denial of service via local access.	5.0	More Details
CVE-2022-46279	Improper access control in the Intel(R) Retail Edge android application before version 3.0.301126-RELEASE may allow an authenticated user to potentially enable information disclosure via local access.	5.0	More Details
CVE-2022-45128	Improper authorization in the Intel(R) EMA software before version 1.9.0.0 may allow an authenticated user to potentially enable denial of service via local access.	5.0	More Details
CVE-2022-43465	Improper authorization in the Intel(R) SCS software all versions may allow an authenticated user to potentially enable denial of service via local access.	5.0	More Details
CVE-2023-25772	Improper input validation in the Intel(R) Retail Edge Mobile Android application before version 3.0.301126-RELEASE may allow an authenticated user to potentially enable denial of service via local access.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31473	An issue was discovered on GL.iNet devices before 3.216. There is an arbitrary file write in which an empty file can be created anywhere on the filesystem. This is caused by a command injection vulnerability with a filter applied. Through the software installation feature, it is possible to inject arbitrary parameters in a request to cause opkg to read an arbitrary file name while using root privileges. The -f option can be used with a configuration file.	4.9	More Details
CVE-2023-30507	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including sensitive system files.	4.9	More Details
CVE-2023-30508	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including sensitive system files.	4.9	More Details
CVE-2023-30509	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including sensitive system files.	4.9	More Details
CVE-2022-41769	Improper access control in the Intel(R) Connect M Android application before version 1.82 may allow an authenticated user to potentially enable escalation of privilege via local access.	4.8	More Details
CVE-2023-31162	An Improper Input Validation vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to arbitrarily alter the content of a configuration file. See SEL Service Bulletin dated 2022-11-15 for more details.	4.8	More Details
CVE-2023-2009	Plugin does not sanitize and escape the URL field in the Pretty Url WordPress plugin through 1.5.4 settings, which could allow high-privilege users 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-2023-1839	The Product Addons & Fields for WooCommerce WordPress plugin before 32.0.6 does not sanitize and escape some of its setting fields, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in multisite setup).	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0892	The BizLibrary WordPress plugin through 1.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-2630	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.21.	4.8	More Details
CVE-2023-23580	Stack-based buffer overflow for some Intel(R) Trace Analyzer and Collector software before version 2021.8.0 published Dec 2022 may allow an authenticated user to potentially escalation of privilege via local access.	4.8	More Details
CVE-2023-32993	Jenkins SAML Single Sign On(SSO) Plugin 2.0.2 and earlier does not perform hostname validation when connecting to miniOrange or the configured IdP to retrieve SAML metadata, which could be abused using a man-in-the-middle attack to intercept these connections.	4.8	More Details
CVE-2023-32068	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In versions prior to 14.10.4 it's possible to exploit well known parameters in XWiki URLs to perform redirection to untrusted site. This vulnerability was partially fixed in the past for XWiki 12.10.7 and 13.3RC1 but there is still the possibility to force specific URLs to skip some checks, e.g. using URLs like `http:example.com` in the parameter would allow the redirect. The issue has now been patched against all patterns that are known for performing redirects. This issue has been patched in XWiki 14.10.4 and 15.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.7	More Details
CVE-2023-29025	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	4.7	More Details
CVE-2023-31151	An Improper Certificate Validation vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote unauthenticated attacker to conduct a man-in-the-middle (MitM) attack. See SEL Service Bulletin dated 2022-11-15 for more details.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29029	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	4.7	More Details
CVE-2023-2515	Mattermost fails to restrict a user with permissions to edit other users and to create personal access tokens from elevating their privileges to system admin	4.7	More Details
CVE-2022-41646	Insufficient control flow management in the Intel(R) IPP Cryptography software before version 2021.6 may allow an unauthenticated user to potentially enable information disclosure via local access.	4.7	More Details
CVE-2023-29022	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	4.7	More Details
CVE-2023-29026	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	4.7	More Details
CVE-2023-29028	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	4.7	More Details
CVE-2022-37409	Insufficient control flow management for the Intel(R) IPP Cryptography software before version 2021.6 may allow an authenticated user to potentially enable information disclosure via local access.	4.7	More Details
CVE-2023-29027	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2646	A vulnerability has been found in TP-Link Archer C7v2 v2_en_us_180114 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component GET Request Parameter Handler. The manipulation leads to denial of service. The attack can only be done within the local network. The associated identifier of this vulnerability is VDB-228775. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.5	More Details
CVE-2023-0008	A file disclosure vulnerability in Palo Alto Networks PAN-OS software enables an authenticated read-write administrator with access to the web interface to export local files from the firewall through a race condition.	4.4	More Details
CVE-2023-23573	Improper access control in the Intel(R) Unite(R) android application before Release 17 may allow a privileged user to potentially enable information disclosure via local access.	4.4	More Details
CVE-2023-20697	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07589148; Issue ID: ALPS07589148.	4.4	More Details
CVE-2023-20711	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07581668; Issue ID: ALPS07581668.	4.4	More Details
CVE-2022-36329	An improper privilege management issue that could allow an attacker to cause a denial of service over the OTA mechanism was discovered in Western Digital My Cloud Home, My Cloud Home Duo and SanDisk ibi devices.This issue affects My Cloud Home and My Cloud Home Duo: before 9.4.0-191; ibi: before 9.4.0-191.	4.4	More Details
CVE-2023-20709	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07576951; Issue ID: ALPS07576951.	4.4	More Details
CVE-2023-20698	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07589144; Issue ID: ALPS07589144.	4.4	More Details
CVE-2023-20719	In pqframework, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629583; Issue ID: ALPS07629583.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20710	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07576935; Issue ID: ALPS07576935.	4.4	More Details
CVE-2023-27863	IBM Spectrum Protect Plus Server 10.1.13, under specific configurations, could allow an elevated user to obtain SMB credentials that may be used to access vSnap data stores. IBM X-Force ID: 249325.	4.4	More Details
CVE-2023-31164	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code. See SEL Service Bulletin dated 2022-11-15 for more details.	4.3	More Details
CVE-2023-31154	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code. See SEL Service Bulletin dated 2022-11-15 for more details.	4.3	More Details
CVE-2023-32999	A missing permission check in Jenkins AppSpider Plugin 1.0.15 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL and send an HTTP POST request with a JSON payload consisting of attacker-specified credentials.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31145	Collabora Online is a collaborative online office suite based on LibreOffice technology. This vulnerability report describes a reflected XSS vulnerability with full CSP bypass in Nextcloud installations using the recommended bundle. The vulnerability can be exploited to perform a trivial account takeover attack. The vulnerability allows attackers to inject malicious code into web pages, which can be executed in the context of the victim's browser session. This means that an attacker can steal sensitive data, such as login credentials or personal information, or perform unauthorized actions on behalf of the victim, such as modifying or deleting data. In this specific case, the vulnerability allows for a trivial account takeover attack. An attacker can exploit the vulnerability to inject code into the victim's browser session, allowing the attacker to take over the victim's account without their knowledge or consent. This can lead to unauthorized access to sensitive information and data, as well as the ability to perform actions on behalf of the victim. Furthermore, the fact that the vulnerability bypasses the Content Security Policy (CSP) makes it more dangerous, as CSP is an important security mechanism used to prevent cross-site scripting attacks. By bypassing CSP, attackers can circumvent the security measures put in place by the web application and execute their malicious code. This issue has been patched in versions 22.05.13, 21.11.9, and 6.4.27. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2023-31153	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code.See SEL Service Bulletin dated 2022-11-15 for more details.	4.3	More Details
CVE-2023-33003	A cross-site request forgery (CSRF) vulnerability in Jenkins Tag Profiler Plugin 0.2 and earlier allows attackers to reset profiler statistics.	4.3	More Details
CVE-2023-33004	A missing permission check in Jenkins Tag Profiler Plugin 0.2 and earlier allows attackers with Overall/Read permission to reset profiler statistics.	4.3	More Details
CVE-2023-2196	A missing permission check in Jenkins Code Dx Plugin 3.1.0 and earlier allows attackers with Item/Read permission to check for the existence of an attacker-specified file path on an agent file system.	4.3	More Details
CVE-2023-2632	Jenkins Code Dx Plugin 3.1.0 and earlier stores Code Dx server API keys unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2633	Jenkins Code Dx Plugin 3.1.0 and earlier does not mask Code Dx server API keys displayed on the configuration form, increasing the potential for attackers to observe and capture them.	4.3	More Details
CVE-2023-2195	A cross-site request forgery (CSRF) vulnerability in Jenkins Code Dx Plugin 3.1.0 and earlier allows attackers to connect to an attacker-specified URL.	4.3	More Details
CVE-2023-2631	A missing permission check in Jenkins Code Dx Plugin 3.1.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL.	4.3	More Details
CVE-2023-31155	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code. See SEL Service Bulletin dated 2022-11-15 for more details.	4.3	More Details
CVE-2023-31165	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code. See SEL Service Bulletin dated 2022-11-15 for more details.	4.3	More Details
CVE-2023-31156	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code. See SEL Service Bulletin dated 2022-11-15 for more details.	4.3	More Details
CVE-2023-31157	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code. See SEL Service Bulletin dated 2022-11-15 for more details.	4.3	More Details
CVE-2023-31158	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code. See SEL Service Bulletin dated 2022-11-15 for more details.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31159	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code. See SEL Service Bulletin dated 2022-11-15 for more details.	4.3	More Details
CVE-2023-32075	The Customer Management Framework (CMF) for Pimcore adds functionality for customer data management. In `pimcore/customer-management-framework-bundle` prior to version 3.3.9, business logic errors are possible in the `Conditions` tab since the counter can be a negative number. This vulnerability is capable of the unlogic in the counter value in the Conditions tab. Users should update to version 3.3.9 to receive a patch or, as a workaround, or apply the patch manually.	4.3	More Details
CVE-2023-31160	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code. See SEL Service Bulletin dated 2022-11-15 for more details.	4.3	More Details
CVE-2023-31163	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code. See SEL Service Bulletin dated 2022-11-15 for more details.	4.3	More Details
CVE-2023-28357	A vulnerability has been identified in Rocket.Chat, where the ACL checks in the Slash Command /mute occur after checking whether a user is a member of a given channel, leaking private channel members to unauthorized users. This allows authenticated users to enumerate whether a username is a member of a channel that they do not have access to.	4.3	More Details
CVE-2023-28360	An omission of security-relevant information vulnerability exists in Brave desktop prior to version 1.48.171 when a user was saving a file there was no download safety check dialog presented to the user.	4.3	More Details
CVE-2023-29927	Versions of Sage 300 through 2022 implement role-based access controls that are only enforced client-side. Low-privileged Sage users, particularly those on a workstation setup in the "Windows Peer-to-Peer Network" or "Client Server Network" Sage 300 configurations, could recover the SQL connection strings being used by Sage 300 and interact directly with the underlying database(s) to create, update, and delete all company records, bypassing the program’s role-based access controls.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22508	Improper Input Validation vulnerability in multiple CODESYS V3 products allows an authenticated remote attacker to block consecutive logins of a specific type.	4.3	More Details
CVE-2023-32996	A missing permission check in Jenkins SAML Single Sign On(SSO) Plugin 2.0.0 and earlier allows attackers with Overall/Read permission to send an HTTP POST request with JSON body containing attacker-specified content, to miniOrange's API for sending emails.	4.3	More Details
CVE-2023-28522	IBM API Connect V10 could allow an authenticated user to perform actions that they should not have access to. IBM X-Force ID: 250585.	4.3	More Details
CVE-2023-0761	The Clock In Portal- Staff & Attendance Management WordPress plugin through 2.1 does not have CSRF check when deleting Staff members, which could allow attackers to make logged in admins delete arbitrary Staff via a CSRF attack	4.3	More Details
CVE-2023-2674	Improper Access Control in GitHub repository openemr/openemr prior to 7.0.1.	4.3	More Details
CVE-2023-2739	A vulnerability classified as problematic was found in Gira HomeServer up to 4.12.0.220829 beta. This vulnerability affects unknown code of the file /hslist. The manipulation of the argument lst with the input debug%27"><img%20src=x%20onerror=alert(document.cookie)> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-229150 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-32978	A cross-site request forgery (CSRF) vulnerability in Jenkins LDAP Plugin allows attackers to connect to an attacker-specified LDAP server using attacker-specified credentials.	4.3	More Details
CVE-2023-32980	A cross-site request forgery (CSRF) vulnerability in Jenkins Email Extension Plugin allows attackers to make another user stop watching an attacker-specified job.	4.3	More Details
CVE-2023-32982	Jenkins Ansible Plugin 204.v8191fd551eb_f and earlier stores extra variables unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32985	Jenkins Sidebar Link Plugin 2.2.1 and earlier does not restrict the path of files in a method implementing form validation, allowing attackers with Overall/Read permission to check for the existence of an attacker-specified file path on the Jenkins controller file system.	4.3	More Details
CVE-2023-32979	Jenkins Email Extension Plugin does not perform a permission check in a method implementing form validation, allowing attackers with Overall/Read permission to check for the existence of files in the email-templates/ directory in the Jenkins home directory on the controller file system.	4.3	More Details
CVE-2023-0763	The Clock In Portal- Staff & Attendance Management WordPress plugin through 2.1 does not have CSRF check when deleting Holidays, which could allow attackers to make logged in admins delete arbitrary holidays via a CSRF attack	4.3	More Details
CVE-2023-32988	A missing permission check in Jenkins Azure VM Agents Plugin 852.v8d35f0960a_43 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2023-0762	The Clock In Portal- Staff & Attendance Management WordPress plugin through 2.1 does not have CSRF check when deleting designations, which could allow attackers to make logged in admins delete arbitrary designations via a CSRF attack	4.3	More Details
CVE-2022-27180	Uncontrolled search path in the Intel(R) MacCPUID software before version 3.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	4.2	More Details
CVE-2023-31166	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to create folders in arbitrary paths of the file system. See SEL Service Bulletin dated 2022-11-15 for more details.	4.1	More Details
CVE-2023-30510	A vulnerability exists in the Aruba EdgeConnect Enterprise web management interface that allows remote authenticated users to issue arbitrary URL requests from the Aruba EdgeConnect Enterprise instance. The impact of this vulnerability is limited to a subset of URLs which can result in the possible disclosure of data due to the network position of the Aruba EdgeConnect Enterprise instance.	4.1	More Details
CVE-2022-38087	Exposure of resource to wrong sphere in BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32970	Auth. (editor+) Stored Cross-Site Scripting (XSS) vulnerability in Themify Themify Portfolio Post plugin <= 1.2.4 versions.	4.1	More Details
CVE-2023-20717	In vcu, there is a possible leak of dma buffer due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645185; Issue ID: ALPS07645185.	4.1	More Details
CVE-2023-29195	Vitess is a database clustering system for horizontal scaling of MySQL through generalized sharding. Prior to version 16.0.2, users can either intentionally or inadvertently create a shard containing `/` characters from VTAdmin such that from that point on, anyone who tries to create a new shard from VTAdmin will receive an error. Attempting to view the keyspace(s) will also no longer work. Creating a shard using `vtctldclient` does not have the same problem because the CLI validates the input correctly. Version 16.0.2, corresponding to version 0.16.2 of the `go` module, contains a patch for this issue. Some workarounds are available. Always use `vtctldclient` to create shards, instead of using VTAdmin; disable creating shards from VTAdmin using RBAC; and/or delete the topology record for the offending shard using the client for your topology server.	4.1	More Details
CVE-2022-33961	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WaspThemes Visual CSS Style Editor plugin <= 7.5.8 versions.	4.0	More Details
CVE-2023-31152	An Authentication Bypass Using an Alternate Path or Channel vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface allows Authentication Bypass. See SEL Service Bulletin dated 2022-11-15 for more details.	4.0	More Details
CVE-2022-31477	Improper initialization for some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable information disclosure via local access.	4.0	More Details
CVE-2023-23910	Out-of-bounds write for some Intel(R) Trace Analyzer and Collector software before version 2021.8.0 published Dec 2022 may allow an authenticated user to potentially escalation of privilege via local access.	3.9	More Details
CVE-2023-32994	Jenkins SAML Single Sign On(SSO) Plugin 2.1.0 and earlier unconditionally disables SSL/TLS certificate validation for connections to miniOrange or the configured IdP to retrieve SAML metadata, which could be abused using a man-in-the-middle attack to intercept these connections.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2691	A vulnerability, which was classified as problematic, was found in SourceCodester Personnel Property Equipment System 1.0. Affected is an unknown function of the file admin/add_item.php of the component POST Parameter Handler. The manipulation of the argument item_name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-228972.	3.5	More Details
CVE-2023-2678	A vulnerability has been found in SourceCodester File Tracker Manager System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /file_manager/admin/save_user.php of the component POST Parameter Handler. The manipulation of the argument firstname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-228892.	3.5	More Details
CVE-2023-2657	A vulnerability classified as problematic was found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this vulnerability is an unknown functionality of the file products.php. The manipulation of the argument search leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-228799.	3.5	More Details
CVE-2023-2692	A vulnerability has been found in SourceCodester ICT Laboratory Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file views/room_info.php of the component GET Parameter Handler. The manipulation of the argument name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-228973 was assigned to this vulnerability.	3.5	More Details
CVE-2023-2667	A vulnerability has been found in SourceCodester Lost and Found Information System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file admin/. The manipulation of the argument page leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-228883.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2671	A vulnerability was found in SourceCodester Lost and Found Information System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file classes/Master.php?f=save_inquiry of the component Contact Form. The manipulation of the argument fullname/contact/message leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-228887.	3.5	More Details
CVE-2023-2740	A vulnerability, which was classified as problematic, has been found in SourceCodester Guest Management System 1.0. Affected by this issue is some unknown functionality of the file dateTest.php of the component GET Parameter Handler. The manipulation of the argument name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229160.	3.5	More Details
CVE-2022-27856	Auth. (editor+) Stored Cross-Site Scripting (XSS) vulnerability in Atlas Gondal Export All URLs plugin <= 4.1 versions.	3.4	More Details
CVE-2022-32577	Improper input validation in BIOS Firmware for some Intel(R) NUC Kits before version PY0081 may allow a privileged user to potentially enable information disclosure or denial of service via local access	3.4	More Details
CVE-2022-41621	Improper access control in some Intel(R) QAT drivers for Windows before version 1.9.0 may allow an authenticated user to potentially enable information disclosure via local access.	3.3	More Details
CVE-2022-41808	Improper buffer restriction in software for the Intel QAT Driver for Linux before version 1.7.l.4.12 may allow an authenticated user to potentially enable denial of service via local access.	3.3	More Details
CVE-2023-20726	In mnld, there is a possible leak of GPS location due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07735968 / ALPS07884552 (For MT6880, MT6890, MT6980, MT6980D and MT6990 only); Issue ID: ALPS07735968 / ALPS07884552 (For MT6880, MT6890, MT6980, MT6980D and MT6990 only).	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0858	Improper Authentication of RemoteUI of Office / Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger unauthorized access to the product. *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe.	3.1	More Details
CVE-2023-32082	etcd is a distributed key-value store for the data of a distributed system. Prior to versions 3.4.26 and 3.5.9, the LeaseTimeToLive API allows access to key names (not value) associated to a lease when `Keys` parameter is true, even a user doesn't have read permission to the keys. The impact is limited to a cluster which enables auth (RBAC). Versions 3.4.26 and 3.5.9 fix this issue. There are no known workarounds.	3.1	More Details
CVE-2023-2662	In Xpdf 4.04 (and earlier), a bad color space object in the input PDF file can cause a divide-by-zero.	2.9	More Details
CVE-2023-2663	In Xpdf 4.04 (and earlier), a PDF object loop in the page label tree leads to infinite recursion and a stack overflow.	2.9	More Details
CVE-2023-2664	In Xpdf 4.04 (and earlier), a PDF object loop in the embedded file tree leads to infinite recursion and a stack overflow.	2.9	More Details
CVE-2023-23909	Out-of-bounds read for some Intel(R) Trace Analyzer and Collector software before version 2021.8.0 published Dec 2022 may allow an authenticated user to potentially enable information disclosure via local access.	2.8	More Details
CVE-2022-42878	Null pointer dereference for some Intel(R) Trace Analyzer and Collector software before version 2021.8.0 published Dec 2022 may allow an authenticated user to potentially enable information disclosure via local access.	2.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0859	Arbitrary Files can be installed in the Setting Data Import function of Office / Small Office Multifunction Printers and Laser Printers(*). *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe.	2.2	More Details
CVE-2023-22447	Insertion of sensitive information into log file in the Open CAS software for Linux maintained by Intel before version 22.6.2 may allow a privileged user to potentially enable information disclosure via local access.	2.0	More Details
CVE-2022-36330	A buffer overflow vulnerability was discovered on firmware version validation that could lead to an unauthenticated remote code execution in Western Digital My Cloud Home, My Cloud Home Duo and SanDisk ibi devices. An attacker would require exploitation of another vulnerability to raise their privileges in order to exploit this buffer overflow vulnerability. This issue affects My Cloud Home and My Cloud Home Duo: before 9.4.0-191; ibi: before 9.4.0-191.	1.9	More Details
CVE-2022-40974	Incomplete cleanup in the Intel(R) IPP Cryptography software before version 2021.6 may allow a privileged user to potentially enable information disclosure via local access.	1.8	More Details
CVE-2023-2511	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-0025	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0016	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0017	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0018	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0019	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0020	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0021	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0022	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0023	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0024	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0026	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0014	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0027	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0028	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0029	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0030	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0031	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0032	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0033	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0034	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0035	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0015	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0011	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0037	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2018-15647	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11788	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11787	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-15654	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2018-15653	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2018-15652	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2018-15651	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2018-15650	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2018-15649	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2018-15648	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2018-15646	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-0010	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2018-15644	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2018-15643	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2018-15642	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-15639	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2018-15637	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2018-15636	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2018-15630	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-31508	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2020-15178. Reason: This record is a duplicate of CVE-2020-15178. Notes: All CVE users should reference CVE-2020-15178 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-31557	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-2664. Reason: This record is a reservation duplicate of CVE-2023-2664. Notes: All CVE users should reference CVE-2023-2664 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2021-0036	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0038	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2023-2510	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-0184	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0137	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0138	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0139	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0140	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0141	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0142	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0149	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0150	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0181	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0191	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0039	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0192	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0195	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-23145	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-26946	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-33065	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-33066	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-33067	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-33070	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2023-31554	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-2663. Reason: This record is a reservation duplicate of CVE-2023-2663. Notes: All CVE users should reference CVE-2023-2663 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2021-0136	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0130	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0128	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0123	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0040	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0041	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0042	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0043	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0044	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0045	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0046	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0047	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0048	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0049	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0050	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0059	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0068	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0080	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0081	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0085	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0087	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0088	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-0122	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2019-11789	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11790	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-11791	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-24944	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-31227	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-2331	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-29101	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-29100	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-29099	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-29088	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-29087	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-29086	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-26853	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24943	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-32479	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-24941	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-24940	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-24427	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-24425	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-23164	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-23162	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-0095	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-0094	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-26674	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-31242	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32494	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11792	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46789	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-2502	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-2501	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-2185	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-0387	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-4853	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-4852	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-48187	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46791	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46790	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46788	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-32495	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46787	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46753	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46681	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-37304	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-37303	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-34461	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-34395	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-33933	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-32496	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-26673	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6608	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6607	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11803	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-29402	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-29401	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-29400	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-29399	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-29398	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-29397	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-6148	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-6141	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-11804	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11802	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6606	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11801	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11800	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11799	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11798	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11797	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11796	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11795	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2019-11794	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-11793	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-29403	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-29404	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-29405	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-29406	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6605	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6604	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6603	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6602	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6601	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6600	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6599	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6598	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6597	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6596	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6595	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6594	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6593	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6592	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6591	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-6589	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-29410	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-29408	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-29407	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32497	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details