SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 16 August 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-2023-40020	PrivateUploader is an open source image hosting server written in Vue and TypeScript. In affected versions `app/routes/v3/admin.controller.ts` did not correctly verify whether the user was an administrator (High Level) or moderator (Low Level) causing the request to continue processing. The response would be a 403 with ADMIN_ONLY, however, next() would call leading to any updates/changes in the route to process. This issue has been addressed in version 3.2.49. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.9	More Details
CVE-2023-39851	webchess v1.0 was discovered to contain a SQL injection vulnerability via the $playerID parameter at mainmenu.php. NOTE: this is disputed by a third party who indicates that the playerID is a session variable controlled by the server, and thus cannot be used for exploitation.	9.8	More Details
CVE-2023-32748	The Linux DVS server component of Mitel MiVoice Connect through 19.3 SP2 (22.24.1500.0) could allow an unauthenticated attacker with internal network access to execute arbitrary scripts due to improper access control.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4322	Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.9.0.	9.8	More Details
CVE-2023-30187	An out of bounds memory access vulnerability in ONLYOFFICE DocumentServer 4.0.3 through 7.3.2 allows remote attackers to run arbitrary code via crafted JavaScript file.	9.8	More Details
CVE-2023-30186	A use after free issue discovered in ONLYOFFICE DocumentServer 4.0.3 through 7.3.2 allows remote attackers to run arbitrary code via crafted JavaScript file.	9.8	More Details
CVE-2023-37847	novel-plus v3.6.2 was discovered to contain a SQL injection vulnerability.	9.8	More Details
CVE-2023-4323	Broadcom RAID Controller web interface is vulnerable to improper session management of active sessions on Gateway setup	9.8	More Details
CVE-2023-3266	A non-feature complete authentication mechanism exists in the production application allowing an attacker to bypass all authentication checks if LDAP authentication is selected.An unauthenticated attacker can leverage this vulnerability to log in to the CypberPower PowerPanel Enterprise as an administrator by selecting LDAP authentication from a hidden HTML combo box. Successful exploitation of this vulnerability also requires the attacker to know at least one username on the device, but any password will authenticate successfully.	9.8	More Details
CVE-2023-3265	An authentication bypass exists on CyberPower PowerPanel Enterprise by failing to sanitize meta-characters from the username, allowing an attacker to login into the application with the default user "cyberpower" by appending a non-printable character.An unauthenticated attacker can leverage this vulnerability to log in to the CypberPower PowerPanel Enterprise as an administrator with hardcoded default credentials.	9.8	More Details
CVE-2023-3259	The Dataprobe iBoot PDU running firmware version 1.43.03312023 or earlier is vulnerable to authentication bypass. By manipulating the IP address field in the "iBootPduSiteAuth" cookie, a malicious agent can direct the device to connect to a rouge database.Successful exploitation allows the malicious agent to take actions with administrator privileges including, but not limited to, manipulating power levels, modifying user accounts, and exporting confidential user information	9.8	More Details
CVE-2023-4324	Broadcom RAID Controller web interface is vulnerable due to insecure defaults of lacking HTTP Content-Security-Policy headers	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4325	Broadcom RAID Controller web interface is vulnerable due to usage of Libcurl with LSA has known vulnerabilities	9.8	More Details
CVE-2023-4329	Broadcom RAID Controller web interface is vulnerable due to insecure default of HTTP configuration that does not safeguard SESSIONID cookie with SameSite attribute	9.8	More Details
CVE-2023-4336	Broadcom RAID Controller web interface is vulnerable due to insecure default of HTTP configuration that does not safeguard cookies with Secure attribute	9.8	More Details
CVE-2023-4337	Broadcom RAID Controller web interface is vulnerable to improper session handling of managed servers on Gateway installation	9.8	More Details
CVE-2023-4338	Broadcom RAID Controller web interface is vulnerable due to insecure default of HTTP configuration that does not provide X-Content-Type-Options Headers	9.8	More Details
CVE-2023-4340	Broadcom RAID Controller is vulnerable to Privilege escalation by taking advantage of the Session prints in the log file	9.8	More Details
CVE-2023-4341	Broadcom RAID Controller is vulnerable to Privilege escalation to root due to creation of insecure folders by Web GUI	9.8	More Details
CVE-2023-40359	xterm before 380 supports ReGIS reporting for character-set names even if they have unexpected characters (i.e., neither alphanumeric nor underscore), aka a pointer/overflow issue. This can only occur for xterm installations that are configured at compile time to use a certain experimental feature.	9.8	More Details
CVE-2023-29468	The Texas Instruments (TI) WiLink WL18xx MCP driver does not limit the number of information elements (IEs) of type XCC_EXT_1_IE_ID or XCC_EXT_2_IE_ID that can be parsed in a management frame. Using a specially crafted frame, a buffer overflow can be triggered that can potentially lead to remote code execution. This affects WILINK8-WIFI-MCP8 version 8.5_SP3 and earlier.	9.8	More Details
CVE-2023-38865	COMFAST CF-XR11 V2.7.2 has a command injection vulnerability detected at function sub_4143F0. Attackers can send POST request messages to /usr/bin/webmgnt and inject commands into parameter timestr.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39292	A SQL Injection vulnerability has been identified in the MiVoice Office 400 SMB Controller through 1.2.5.23 which could allow a malicious actor to access sensitive information and execute arbitrary database and management operations.	9.8	More Details
CVE-2023-38862	An issue in COMFAST CF-XR11 v.2.7.2 allows an attacker to execute arbitrary code via the destination parameter of sub_431F64 function in bin/webmgnt.	9.8	More Details
CVE-2023-38861	An issue in Wavlink WL_WNJ575A3 v.R75A3_V1410_220513 allows a remote attacker to execute arbitrary code via username parameter of the set_sys_adm function in adm.cgi.	9.8	More Details
CVE-2023-39662	An issue in llama_index v.0.7.13 and before allows a remote attacker to execute arbitrary code via the `exec` parameter in PandasQueryEngine function.	9.8	More Details
CVE-2023-39661	An issue in pandas-ai v.0.9.1 and before allows a remote attacker to execute arbitrary code via the _is_jailbreak function.	9.8	More Details
CVE-2023-39659	An issue in langchain langchain-ai v.0.0.232 and before allows a remote attacker to execute arbitrary code via a crafted script to the PythonAstREPLTool._run component.	9.8	More Details
CVE-2023-38915	File Upload vulnerability in Wolf-leo EasyAdmin8 v.1.0 allows a remote attacker to execute arbtirary code via the upload type function.	9.8	More Details
CVE-2023-38896	An issue in Harrison Chase langchain v.0.0.194 and before allows a remote attacker to execute arbitrary code via the from_math_prompt and from_colored_object_prompt functions.	9.8	More Details
CVE-2023-38889	An issue in Alluxio v.2.9.3 and before allows an attacker to execute arbitrary code via a crafted script to the username parameter of lluxio.util.CommonUtils.getUnixGroups(java.lang.String).	9.8	More Details
CVE-2023-38860	An issue in LangChain v.0.0.231 allows a remote attacker to execute arbitrary code via the prompt parameter.	9.8	More Details
CVE-2023-35082	An authentication bypass vulnerability in Ivanti EPMM 11.10 and older, allows unauthorized users to access restricted functionality or resources of the application without proper authentication. This vulnerability is unique to CVE-2023-35078 announced earlier.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21287	In multiple locations, there is a possible code execution due to type confusion. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-21242	In isServerCertChainValid of InsecureEapNetworkHandler.java, there is a possible way to trust an imposter server due to a logic error in the code. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-20965	In processMessageImpl of ClientModeImpl.java, there is a possible credential disclosure in the TOFU flow due to a logic error in the code. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-3435	The User Activity Log WordPress plugin before 1.6.5 does not correctly sanitise and escape several parameters before using it in a SQL statement as part of its exportation feature, allowing unauthenticated attackers to conduct SQL injection attacks.	9.8	More Details
CVE-2023-39293	A Command Injection vulnerability has been identified in the MiVoice Office 400 SMB Controller through 1.2.5.23 which could allow a malicious actor to execute arbitrary commands within the context of the system.	9.8	More Details
CVE-2023-39405	Vulnerability of out-of-bounds parameter read/write in the Wi-Fi module. Successful exploitation of this vulnerability may cause other apps to be executed with escalated privileges.	9.8	More Details
CVE-2023-3452	The Canto plugin for WordPress is vulnerable to Remote File Inclusion in versions up to, and including, 3.0.4 via the 'wp_abspath' parameter. This allows unauthenticated attackers to include and execute arbitrary remote code on the server, provided that allow_url_include is enabled. Local File Inclusion is also possible, albeit less useful because it requires that the attacker be able to upload a malicious php file via FTP or some other means into a directory readable by the web server.	9.8	More Details
CVE-2021-28411	An issue was discovered in getRememberedSerializedIdentity function in CookieRememberMeManager class in lerry903 RuoYi version 3.4.0, allows remote attackers to escalate privileges.	9.8	More Details
CVE-2023-37068	Code-Projects Gym Management System V1.0 allows remote attackers to execute arbitrary SQL commands via the login form, leading to unauthorized access and potential data manipulation. This vulnerability arises due to insufficient validation of user-supplied input in the username and password fields, enabling SQL Injection attacks.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32567	Ivanti Avalanche decodeToMap XML External Entity Processing. Fixed in version 6.4.1.236	9.8	More Details
CVE-2023-38866	COMFAST CF-XR11 V2.7.2 has a command injection vulnerability detected at function sub_415588. Attackers can send POST request messages to /usr/bin/webmgnt and inject commands into parameter interface and display_name.	9.8	More Details
CVE-2023-36311	There is a SQL injection (SQLi) vulnerability in the "column" parameter of index.php in PHPJabbers Document Creator v1.0.	9.8	More Details
CVE-2023-39776	A File Upload vulnerability in PHPJabbers Ticket Support Script v3.2 allows attackers to execute arbitrary code via uploading a crafted file.	9.8	More Details
CVE-2023-37734	EZ softmagic MP3 Audio Converter 2.7.3.700 was discovered to contain a buffer overflow.	9.8	More Details
CVE-2023-37069	Code-Projects Online Hospital Management System V1.0 is vulnerable to SQL Injection (SQLI) attacks, which allow an attacker to manipulate the SQL queries executed by the application. The application fails to properly validate user-supplied input in the login id and password fields during the login process, enabling an attacker to inject malicious SQL code.	9.8	More Details
CVE-2023-39852	Doctormms v1.0 was discovered to contain a SQL injection vulnerability via the $userid parameter at myAppoinment.php. NOTE: this is disputed by a third party who claims that the userid is a session variable controlled by the server, and thus cannot be used for exploitation. The original reporter counterclaims that this originates from $_SESSION["userid"]=$_POST["userid"] at line 68 in doctors\doctorlogin.php, where userid under POST is not a session variable controlled by the server.	9.8	More Details
CVE-2023-38034	A command injection vulnerability in the DHCP Client function of all UniFi Access Points and Switches, excluding the Switch Flex Mini, could allow a Remote Code Execution (RCE). Affected Products: All UniFi Access Points (Version 6.5.53 and earlier) All UniFi Switches (Version 6.5.32 and earlier) - USW Flex Mini excluded. Mitigation: Update UniFi Access Points to Version 6.5.62 or later. Update UniFi Switches to Version 6.5.59 or later.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39008	A command injection vulnerability in the component /api/cron/settings/setJob/ of OPNsense Community Edition before 23.7 and Business Edition before 23.4.2 allows attackers to execute arbitrary system commands.	9.8	More Details
CVE-2023-39004	Insecure permissions in the configuration directory (/conf/) of OPNsense Community Edition before 23.7 and Business Edition before 23.4.2 allow attackers to access sensitive information (e.g., hashed root password) which could lead to privilege escalation.	9.8	More Details
CVE-2023-39001	A command injection vulnerability in the component diag_backup.php of OPNsense Community Edition before 23.7 and Business Edition before 23.4.2 allows attackers to execute arbitrary commands via a crafted backup configuration file.	9.8	More Details
CVE-2023-39850	Schoolmate v1.3 was discovered to contain multiple SQL injection vulnerabilities via the $courseid and $teacherid parameters at DeleteFunctions.php.	9.8	More Details
CVE-2023-34545	A SQL injection vulnerability in CSZCMS 1.3.0 allows remote attackers to run arbitrary SQL commands via p parameter or the search URL.	9.8	More Details
CVE-2023-3632	Use of Hard-coded Cryptographic Key vulnerability in Sifir Bes Education and Informatics Kunduz - Homework Helper App allows Authentication Abuse, Authentication Bypass.This issue affects Kunduz - Homework Helper App: before 6.2.3.	9.8	More Details
CVE-2021-27523	An issue was discovered in open-falcon dashboard version 0.2.0, allows remote attackers to gain, modify, and delete sensitive information via crafted POST request to register interface.	9.8	More Details
CVE-2023-35085	An integer overflow vulnerability in all UniFi Access Points and Switches, excluding the Switch Flex Mini, with SNMP Monitoring and default settings enabled could allow a Remote Code Execution (RCE). Affected Products: All UniFi Access Points (Version 6.5.50 and earlier) All UniFi Switches (Version 6.5.32 and earlier) -USW Flex Mini excluded. Mitigation: Update UniFi Access Points to Version 6.5.62 or later. Update the UniFi Switches to Version 6.5.59 or later.	9.8	More Details
CVE-2023-32560	An attacker can send a specially crafted message to the Wavelink Avalanche Manager, which could result in service disruption or arbitrary code execution. Thanks to a Researcher at Tenable for finding and reporting. Fixed in version 6.4.1.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32562	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.3.x and below that could allow an attacker to achieve a remove code execution. Fixed in version 6.4.1.	9.8	More Details
CVE-2021-26505	Prototype pollution vulnerability in MrSwitch hello.js version 1.18.6, allows remote attackers to execute arbitrary code via hello.utils.extend function.	9.8	More Details
CVE-2020-36082	File Upload vulnerability in bloofoxCMS version 0.5.2.1, allows remote attackers to execute arbitrary code and escalate privileges via crafted webshell file to upload module.	9.8	More Details
CVE-2020-36034	SQL Injection vulnerability in oretnom23 School Faculty Scheduling System version 1.0, allows remote attacker to execute arbitrary code, escalate privilieges, and gain sensitive information via crafted payload to id parameter in manage_user.php.	9.8	More Details
CVE-2020-27544	An issue was discovered in FoldingAtHome Client Advanced Control GUI before commit 9b619ae64443997948a36dda01b420578de1af77, allows remote attackers to execute arbitrary code via crafted payload to function parse_message in file Connection.py.	9.8	More Details
CVE-2023-4342	Broadcom RAID Controller web interface is vulnerable due to insecure defaults of lacking HTTP strict-transport-security policy	9.8	More Details
CVE-2023-40267	GitPython before 3.1.32 does not block insecure non-multi options in clone and clone_from. NOTE: this issue exists because of an incomplete fix for CVE-2022-24439.	9.8	More Details
CVE-2023-4344	Broadcom RAID Controller web interface is vulnerable to insufficient randomness due to improper use of ssl.rnd to setup CIM connection	9.8	More Details
CVE-2023-38863	An issue in COMFAST CF-XR11 v.2.7.2 allows an attacker to execute arbitrary code via the ifname and mac parameters in the sub_410074 function at bin/webmgnt.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40256	A vulnerability was discovered in Veritas NetBackup Snapshot Manager before 10.2.0.1 that allowed untrusted clients to interact with the RabbitMQ service. This was caused by improper validation of the client certificate due to misconfiguration of the RabbitMQ service. Exploiting this impacts the confidentiality and integrity of messages controlling the backup and restore jobs, and could result in the service becoming unavailable. This impacts only the jobs controlling the backup and restore activities, and does not allow access to (or deletion of) the backup snapshot data itself. This vulnerability is confined to the NetBackup Snapshot Manager feature and does not impact the RabbitMQ instance on the NetBackup primary servers.	9.8	More Details
CVE-2023-39806	iCMS v7.0.16 was discovered to contain a SQL injection vulnerability via the bakupdata function.	9.8	More Details
CVE-2023-39805	iCMS v7.0.16 was discovered to contain a SQL injection vulnerability via the where parameter at admincp.php.	9.8	More Details
CVE-2023-38864	An issue in COMFAST CF-XR11 v.2.7.2 allows an attacker to execute arbitrary code via the protal_delete_picname parameter in the sub_41171C function at bin/webmgnt.	9.8	More Details
CVE-2023-32564	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.4.1 and below that could allow an attacker to achieve a remove code execution.	9.8	More Details
CVE-2023-32563	An unauthenticated attacker could achieve the code execution through a RemoteControl server.	9.8	More Details
CVE-2023-33241	Crypto wallets implementing the GG18 or GG20 TSS protocol might allow an attacker to extract a full ECDSA private key by injecting a malicious pallier key and cheating in the range proof. Depending on the Beta parameters chosen in the protocol implementation, the attack might require 16 signatures or more fully exfiltrate the other parties' private key shares.	9.6	More Details
CVE-2023-33242	Crypto wallets implementing the Lindell17 TSS protocol might allow an attacker to extract the full ECDSA private key by exfiltrating a single bit in every signature attempt (256 in total) because of not adhering to the paper's security proof's assumption regarding handling aborts after a failed signature.	9.6	More Details
CVE-2023-39007	/ui/cron/item/open in the Cron component of OPNsense Community Edition before 23.7 and Business Edition before 23.4.2 allows XSS via openAction in app/controllers/OPNsense/Cron/ItemController.php.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3824	In PHP version 8.0.* before 8.0.30, 8.1.* before 8.1.22, and 8.2.* before 8.2.8, when loading phar file, while reading PHAR directory entries, insufficient length checking may lead to a stack buffer overflow, leading potentially to memory corruption or RCE.	9.4	More Details
CVE-2023-33934	Improper Input Validation vulnerability in Apache Software Foundation Apache Traffic Server.This issue affects Apache Traffic Server: through 9.2.1.	9.1	More Details
CVE-2023-3267	When adding a remote backup location, an authenticated user can pass arbitrary OS commands through the username field. The username is passed without sanitization into CMD running as NT/Authority System. An authenticated attacker can leverage this vulnerability to execute arbitrary code with system-level access to the CyberPower PowerPanel Enterprise server.	9.1	More Details
CVE-2023-39403	Parameter verification vulnerability in the installd module. Successful exploitation of this vulnerability may cause sandbox files to be read and written without authorization.	9.1	More Details
CVE-2023-38208	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead to arbitrary code execution by an admin-privilege authenticated attacker. Exploitation of this issue does not require user interaction.	9.1	More Details
CVE-2023-39401	Parameter verification vulnerability in the installd module. Successful exploitation of this vulnerability may cause sandbox files to be read and written without authorization.	9.1	More Details
CVE-2023-39400	Parameter verification vulnerability in the installd module. Successful exploitation of this vulnerability may cause sandbox files to be read and written without authorization.	9.1	More Details
CVE-2023-39399	Parameter verification vulnerability in the installd module. Successful exploitation of this vulnerability may cause sandbox files to be read and written without authorization.	9.1	More Details
CVE-2023-39398	Parameter verification vulnerability in the installd module. Successful exploitation of this vulnerability may cause sandbox files to be read and written without authorization.	9.1	More Details
CVE-2023-39385	Vulnerability of configuration defects in the media module of certain products.. Successful exploitation of this vulnerability may cause unauthorized access.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46895	Vulnerability of defects introduced in the design process in the Multi-Device Task Center. Successful exploitation of this vulnerability will cause the hopped app to bypass the app lock and reset the device that initiates the hop.	9.1	More Details
CVE-2020-27514	Directory Traversal vulnerability in delete function in admin.api.TemplateController in ZrLog version 2.1.15, allows remote attackers to delete arbitrary files and cause a denial of service (DoS).	9.1	More Details
CVE-2023-40260	EmpowerID before 7.205.0.1 allows an attacker to bypass an MFA (multi factor authentication) requirement if the first factor (username and password) is known, because the first factor is sufficient to change an account's email address, and the product would then send MFA codes to the new email address (which may be attacker-controlled). NOTE: this is different from CVE-2023-4177, which claims to be about "some unknown processing of the component Multi-Factor Authentication Code Handler" and thus cannot be correlated with other vulnerability information.	9.1	More Details
CVE-2023-32565	An attacker can send a specially crafted request which could lead to leakage of sensitive data or potentially a resource-based DoS attack. Fixed in version 6.4.1.	9.1	More Details
CVE-2023-32566	An attacker can send a specially crafted request which could lead to leakage of sensitive data or potentially a resource-based DoS attack. Fixed in version 6.4.1.	9.1	More Details
CVE-2023-33468	KramerAV VIA Connect (2) and VIA Go (2) devices with a version prior to 4.0.1.1326 exhibit a vulnerability that enables remote manipulation of the device. This vulnerability involves extracting the connection confirmation code remotely, bypassing the need to obtain it directly from the physical screen.	9.1	More Details
CVE-2023-39402	Parameter verification vulnerability in the installd module. Successful exploitation of this vulnerability may cause sandbox files to be read and written without authorization.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39969	uthenticode is a small cross-platform library for partially verifying Authenticode digital signatures. Version 1.0.9 of uthenticode hashed the entire file rather than hashing sections by virtual address, in violation of the Authenticode specification. As a result, an attacker could modify code within a binary without changing its Authenticode hash, making it appear valid from uthenticode's perspective. Versions of uthenticode prior to 1.0.9 are not vulnerable to this attack, nor are versions in the 2.x series. By design, uthenticode does not perform full-chain validation. However, the malleability of signature verification introduced in 1.0.9 was an unintended oversight. The 2.x series addresses the vulnerability. Versions prior to 1.0.9 are also not vulnerable, but users are encouraged to upgrade rather than downgrade. There are no workarounds to this vulnerability.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-48597	A SQL injection vulnerability exists in the “ticket event report” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48592	A SQL injection vulnerability exists in the vendor_country parameter of the “vendor print report” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48601	A SQL injection vulnerability exists in the “network print report” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48600	A SQL injection vulnerability exists in the “notes view” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48599	A SQL injection vulnerability exists in the “reporter events type” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48598	A SQL injection vulnerability exists in the “reporter events type date” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48596	A SQL injection vulnerability exists in the “ticket queue watchers” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48595	A SQL injection vulnerability exists in the “ticket template watchers” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48594	A SQL injection vulnerability exists in the “ticket watchers email” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48593	A SQL injection vulnerability exists in the “topology data service” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48591	A SQL injection vulnerability exists in the vendor_state parameter of the “vendor print report” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48580	A command injection vulnerability exists in the ARP ping device tool feature of the ScienceLogic SL1 that takes unsanitized user controlled input and passes it directly to a shell command. This allows for the injection of arbitrary commands to the underlying operating system.	8.8	More Details
CVE-2022-48590	A SQL injection vulnerability exists in the “admin dynamic app mib errors” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48589	A SQL injection vulnerability exists in the “reporting job editor” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48587	A SQL injection vulnerability exists in the “schedule editor” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48586	A SQL injection vulnerability exists in the “json walker” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48585	A SQL injection vulnerability exists in the “admin brand portal” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48584	A command injection vulnerability exists in the download and convert report feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a shell command. This allows for the injection of arbitrary commands to the underlying operating system.	8.8	More Details
CVE-2022-48583	A command injection vulnerability exists in the dashboard scheduler feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a shell command. This allows for the injection of arbitrary commands to the underlying operating system.	8.8	More Details
CVE-2022-48582	A command injection vulnerability exists in the ticket report generate feature of the ScienceLogic SL1 that takes unsanitized user controlled input and passes it directly to a shell command. This allows for the injection of arbitrary commands to the underlying operating system.	8.8	More Details
CVE-2022-48602	A SQL injection vulnerability exists in the “message viewer print” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48603	A SQL injection vulnerability exists in the “message viewer iframe” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2022-48604	A SQL injection vulnerability exists in the “logging export” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21282	In TRANSPOSER_SETTINGS of lpp_tran.h, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.	8.8	More Details
CVE-2022-42828	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	8.8	More Details
CVE-2023-28483	An issue was discovered in Tigergraph Enterprise 3.7.0. The GSQL query language provides users with the ability to write data to files on a remote TigerGraph server. The locations that a query is allowed to write to are configurable via the GSQL.FileOutputPolicy configuration setting. GSQL queries that contain UDFs can bypass this configuration setting and, as a consequence, can write to any file location to which the administrative user has access.	8.8	More Details
CVE-2023-28481	An issue was discovered in Tigergraph Enterprise 3.7.0. There is unsecured write access to SSH authorized keys file. Any code running as the tigergraph user is able to add their SSH public key into the authorised keys file. This allows an attacker to obtain password-less SSH key access by using their own SSH key.	8.8	More Details
CVE-2023-33013	A post-authentication command injection vulnerability in the NTP feature of Zyxel NBG6604 firmware version V1.01(ABIR.1)C0 could allow an authenticated attacker to execute some OS commands remotely by sending a crafted HTTP request.	8.8	More Details
CVE-2023-4369	Insufficient data validation in Systems Extensions in Google Chrome on ChromeOS prior to 116.0.5845.120 allowed an attacker who convinced a user to install a malicious extension to bypass file restrictions via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2022-48503	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 15.6, watchOS 8.7, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5, Safari 15.6. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-28198	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 16.4 and iPadOS 16.4, macOS Ventura 13.3. Processing web content may lead to arbitrary code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4276	The Absolute Privacy plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.1. This is due to missing nonce validation on the 'abpr_profileShortcode' function. This makes it possible for unauthenticated attackers to change user email and password via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2023-40295	libboron in Boron 2.0.8 has a heap-based buffer overflow in ur_strInitUtf8 at string.c.	8.8	More Details
CVE-2023-32358	A type confusion issue was addressed with improved checks. This issue is fixed in iOS 16.4 and iPadOS 16.4, macOS Ventura 13.3. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-4277	The Realia plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.4.0. This is due to missing nonce validation on the 'process_change_profile_form' function. This makes it possible for unauthenticated attackers to change user email via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2023-38348	A CSRF issue was discovered in LWsystems Benno MailArchiv 2.10.1.	8.8	More Details
CVE-2023-28479	An issue was discovered in Tigergraph Enterprise 3.7.0. The TigerGraph platform installs a full development toolchain within every TigerGraph deployment. An attacker is able to compile new executables on each Tigergraph system and modify system and Tigergraph binaries.	8.8	More Details
CVE-2023-32004	A vulnerability has been discovered in Node.js version 20, specifically within the experimental permission model. This flaw relates to improper handling of Buffers in file system APIs causing a traversal path to bypass when verifying file permissions. This vulnerability affects all users using the experimental permission model in Node.js 20. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.	8.8	More Details
CVE-2023-32006	The use of `module.constructor.createRequire()` can bypass the policy mechanism and require modules outside of the policy.json definition for a given module. This vulnerability affects all users using the experimental policy mechanism in all active release lines: 16.x, 18.x, and, 20.x. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4293	The Premium Packages - Sell Digital Products Securely plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 5.7.4 due to insufficient restriction on the 'wpdmpp_update_profile' function. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to modify their user role by supplying the 'profile[role]' parameter during a profile update.	8.8	More Details
CVE-2023-31209	Improper neutralization of active check command arguments in Checkmk < 2.1.0p32, < 2.0.0p38, < 2.2.0p4 leads to arbitrary command execution for authenticated users.	8.8	More Details
CVE-2022-48581	A command injection vulnerability exists in the “dash export” feature of the ScienceLogic SL1 that takes unsanitized user controlled input and passes it directly to a shell command. This allows for the injection of arbitrary commands to the underlying operating system.	8.8	More Details
CVE-2022-48588	A SQL injection vulnerability exists in the “schedule editor decoupled” feature of the ScienceLogic SL1 that takes unsanitized user-controlled input and passes it directly to a SQL query. This allows for the injection of arbitrary SQL before being executed against the database.	8.8	More Details
CVE-2023-21273	In SDP_AddAttribute of sdp_db.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	8.8	More Details
CVE-2023-4351	Use after free in Network in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who has elicited a browser shutdown to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-4352	Type confusion in V8 in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-4353	Heap buffer overflow in ANGLE in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2020-36037	An issue was disocvered in wuzhicms version 4.1.0, allows remote attackers to execte arbitrary code via the setting parameter to the ueditor in index.php.	8.8	More Details
CVE-2020-28848	CSV Injection vulnerability in ChurchCRM version 4.2.0, allows remote attackers to execute arbitrary code via crafted CSV file.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37861	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated remote attacker can execute code with root permissions with a specially crafted HTTP POST when uploading a certificate to the device.	8.8	More Details
CVE-2023-28380	Uncontrolled search path for the Intel(R) AI Hackathon software before version 2.0.0 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	8.8	More Details
CVE-2023-4358	Use after free in DNS in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2020-23595	Cross Site Request Forgery (CSRF) vulnerability in yzmcms version 5.6, allows remote attackers to escalate privileges and gain sensitive information sitemodel/add.html endpoint.	8.8	More Details
CVE-2023-4243	The FULL - Customer plugin for WordPress is vulnerable to Arbitrary File Upload via the /install-plugin REST route in versions up to, and including, 2.2.3 due to improper authorization. This allows authenticated attackers with subscriber-level permissions and above to execute code by installing plugins from arbitrary remote locations including non-repository sources onto the site, granted they are packaged as a valid WordPress plugin.	8.8	More Details
CVE-2023-4354	Heap buffer overflow in Skia in Google Chrome prior to 116.0.5845.96 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-2023-2905	Due to a failure in validating the length of a provided MQTT_CMD_PUBLISH parsed message with a variable length header, Cesanta Mongoose, an embeddable web server, version 7.10 is susceptible to a heap-based buffer overflow vulnerability in the default configuration. Version 7.9 and prior does not appear to be vulnerable. This issue is resolved in version 7.11.	8.8	More Details
CVE-2023-4355	Out of bounds memory access in V8 in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-4356	Use after free in Audio in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who has convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24922	Cross Site Request Forgery (CSRF) vulnerability in xxl-job-admin/user/add in xuxueli xxl-job version 2.2.0, allows remote attackers to execute arbitrary code and esclate privileges via crafted .html file.	8.8	More Details
CVE-2023-4357	Insufficient validation of untrusted input in XML in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-23574	A blind SQL Injection vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in the alerts_count component, allows an authenticated attacker to execute arbitrary SQL statements on the DBMS used by the web application. Authenticated users may be able to extract arbitrary information from the DBMS in an uncontrolled way, alter its structure and data, and/or affect its availability.	8.8	More Details
CVE-2023-22378	A blind SQL Injection vulnerability in Nozomi Networks Guardian and CMC, due to improper input validation in the sorting parameter, allows an authenticated attacker to execute arbitrary SQL statements on the DBMS used by the web application. Authenticated users may be able to extract arbitrary information from the DBMS in an uncontrolled way, alter its structure and data, and/or affect its availability.	8.8	More Details
CVE-2020-24950	SQL Injection vulnerability in file Base_module_model.php in Daylight Studio FUEL-CMS version 1.4.9, allows remote attackers to execute arbitrary code via the col parameter to function list_items.	8.8	More Details
CVE-2023-4368	Insufficient policy enforcement in Extensions API in Google Chrome prior to 116.0.5845.96 allowed an attacker who convinced a user to install a malicious extension to bypass an enterprise policy via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-31452	A cross-site request forgery (CSRF) token bypass was identified in PRTG 23.2.84.1566 and earlier versions that allows remote attackers to perform actions with the permissions of a victim user, provided the victim user has an active session and is induced to trigger the malicious request. This could force PRTG to execute different actions, such as creating new users. The severity of this vulnerability is high and received a score of 8.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8	More Details
CVE-2023-4362	Heap buffer overflow in Mojom IDL in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who had compromised the renderer process and gained control of a WebUI process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4349	Use after free in Device Trust Connectors in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2021-29378	SQL Injection in pear-admin-think version 2.1.2, allows attackers to execute arbitrary code and escalate privileges via crafted GET request to Crud.php.	8.8	More Details
CVE-2023-4239	The Real Estate Manager plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 6.7.1 due to insufficient restriction on the 'rem_save_profile_front' function. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to modify their user role by supplying the 'wp_capabilities' parameter during a profile update.	8.8	More Details
CVE-2023-38916	SQL Injection vulnerability in eVotingSystem-PHP v.1.0 allows a remote attacker to execute arbitrary code and obtain sensitive information via the user input fields.	8.8	More Details
CVE-2023-2312	Use after free in Offline in Google Chrome on Android prior to 116.0.5845.96 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-2023-4366	Use after free in Extensions in Google Chrome prior to 116.0.5845.96 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: Medium)	8.8	More Details
CVE-2022-36392	Improper input validation in some firmware for Intel(R) AMT and Intel(R) Standard Manageability before versions 11.8.94, 11.12.94, 11.22.94, 12.0.93, 14.1.70, 15.0.45, and 16.1.27 in Intel (R) CSME may allow an unauthenticated user to potentially enable denial of service via network access.	8.6	More Details
CVE-2023-3823	In PHP versions 8.0.* before 8.0.30, 8.1.* before 8.1.22, and 8.2.* before 8.2.8 various XML functions rely on libxml global state to track configuration variables, like whether external entities are loaded. This state is assumed to be unchanged unless the user explicitly changes it by calling appropriate function. However, since the state is process-global, other modules - such as ImageMagick - may also use this library within the same process, and change that global state for their internal purposes, and leave it in a state where external entities loading is enabled. This can lead to the situation where external XML is parsed with external entities loaded, which can lead to disclosure of any local files accessible to PHP. This vulnerable state may persist in the same process across many requests, until the process is shut down.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38721	The IBM i 7.2, 7.3, 7.4, and 7.5 product Facsimile Support for i contains a local privilege escalation vulnerability. A malicious actor could gain access to a command line with elevated privileges allowing root access to the host operating system. IBM X-Force ID: 262173.	8.4	More Details
CVE-2023-30691	Parcel mismatch in AuthenticationConfig prior to SMR Aug-2023 Release 1 allows local attacker to privilege escalation.	8.4	More Details
CVE-2023-30680	Improper privilege management vulnerability in MMIGroup prior to SMR Aug-2023 Release 1 allows code execution with privilege.	8.4	More Details
CVE-2022-46329	Protection mechanism failure for some Intel(R) PROSet/Wireless WiFi software may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2023-37862	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an unauthenticated remote attacker can access upload-functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service.	8.2	More Details
CVE-2023-34086	Improper input validation in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2022-27635	Improper access control for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi software may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2023-39945	eprosima Fast DDS is a C++ implementation of the Data Distribution Service standard of the Object Management Group. Prior to versions 2.11.0, 2.10.2, 2.9.2, and 2.6.5, a data submessage sent to PDP port raises unhandled `BadParamException` in fastcdr, which in turn crashes fastdds. Versions 2.11.0, 2.10.2, 2.9.2, and 2.6.5 contain a patch for this issue.	8.2	More Details
CVE-2023-32617	Improper input validation in some Intel(R) NUC Rugged Kit, Intel(R) NUC Kit and Intel(R) Compute Element BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39946	eprosima Fast DDS is a C++ implementation of the Data Distribution Service standard of the Object Management Group. Prior to versions 2.11.1, 2.10.2, 2.9.2, and 2.6.6, heap can be overflowed by providing a PID_PROPERTY_LIST parameter that contains a CDR string with length larger than the size of actual content. In `eprosima::fastdds::dds::ParameterPropertyList_t::push_back_helper`, `memcpy` is called to first copy the octet'ized length and then to copy the data into `properties_.data`. At the second memcpy, both `data` and `size` can be controlled by anyone that sends the CDR string to the discovery multicast port. This can remotely crash any Fast-DDS process. Versions 2.11.1, 2.10.2, 2.9.2, and 2.6.6 contain a patch for this issue.	8.2	More Details
CVE-2023-39947	eprosima Fast DDS is a C++ implementation of the Data Distribution Service standard of the Object Management Group. Prior to versions 2.11.1, 2.10.2, 2.9.2, and 2.6.6, even after the fix at commit 3492270, malformed `PID_PROPERTY_LIST` parameters cause heap overflow at a different program counter. This can remotely crash any Fast-DDS process. Versions 2.11.1, 2.10.2, 2.9.2, and 2.6.6 contain a patch for this issue.	8.2	More Details
CVE-2023-28714	Improper access control in firmware for some Intel(R) PROSet/Wireless WiFi software for Windows before version 22.220 HF (Hot Fix) may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2023-28385	Improper authorization in the Intel(R) NUC Pro Software Suite for Windows before version 2.0.0.9 may allow a privileged user to potentially enable escalation of privilage via local access.	8.2	More Details
CVE-2023-0872	The Horizon REST API includes a users endpoint in OpenMNS Horizon 31.0.8 and versions earlier than 32.0.2 on multiple platforms is vulnerable to elevation of privilege. The solution is to upgrade to Meridian 2023.1.6, 2022.1.19, 2021.1.30, 2020.1.38 or Horizon 32.0.2 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. OpenNMS thanks Erik Wynter for reporting this issue.	8.2	More Details
CVE-2023-27515	Cross-site scripting (XSS) for the Intel(R) DSA software before version 23.1.9 may allow unauthenticated user to potentially enable escalation of privilege via network access.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39963	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 20.0.0 and prior to versions 20.0.14.15, 21.0.9.13, 22.2.10.14, 23.0.12.8, 24.0.12.5, 25.0.9, 26.0.4, and 27.0.1, a missing password confirmation allowed an attacker, after successfully stealing a session from a logged in user, to create app passwords for the victim. Nextcloud server versions 25.0.9, 26.0.4, and 27.0.1 and Nextcloud Enterprise Server versions 20.0.14.15, 21.0.9.13, 22.2.10.14, 23.0.12.9, 24.0.12.5, 25.0.9, 26.0.4, and 27.0.1 contain a patch for this issue. No known workarounds are available.	8.1	More Details
CVE-2022-29887	Cross-site Scripting (XSS) in some Intel(R) Manageability Commander software before version 2.3 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	8.1	More Details
CVE-2023-39438	A missing authorization check allows an arbitrary authenticated user to perform certain operations through the API of CLA-assistant by executing specific additional steps. This allows an arbitrary authenticated user to read CLA information including information of the persons who signed them as well as custom fields the CLA requester had configured. In addition, an arbitrary authenticated user can update or delete the CLA-configuration for repositories or organizations using CLA-assistant. The stored access tokens for GitHub are not affected, as these are redacted from the API-responses.	8.1	More Details
CVE-2022-37336	Improper input validation in BIOS firmware for some Intel(R) NUC may allow a privileged user to potentially enable escalation of privilege via local access.	7.9	More Details
CVE-2022-40964	Improper access control for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi software may allow a privileged user to potentially enable escalation of privilege via local access.	7.9	More Details
CVE-2023-38223	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer 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-2023-38222	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use After Free 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 Number	Description	Base Score	Reference
CVE-2023-38224	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use After Free 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-2023-38225	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use After Free 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-2023-38226	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-29320	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Violation of Secure Design Principles vulnerability that could result in arbitrary code execution in the context of the current user by bypassing the API blacklisting feature. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-21229	In registerServiceLocked of ManagedServices.java, there is a possible bypass of background activity launch restrictions due to an unsafe PendingIntent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-21269	In startActivityInner of ActivityStarter.java, there is a possible way to launch an activity into PiP mode from the background due to BAL bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-38229	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read 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-2023-38227	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use After Free 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 Number	Description	Base Score	Reference
CVE-2023-38228	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use After Free 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-2023-38234	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2023-38231	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-38233	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-38246	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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-2022-47636	A DLL hijacking vulnerability has been discovered in OutSystems Service Studio 11 11.53.30 build 61739. When a user open a .oml file (OutSystems Modeling Language), the application will load the following DLLs from the same directory av_libGLESv2.dll, libcef.DLL, user32.dll, and d3d10warp.dll. Using a crafted DLL, it is possible to execute arbitrary code in the context of the current logged in user.	7.8	More Details
CVE-2023-39957	Nextcloud Talk Android allows users to place video and audio calls through Nextcloud on Android. Prior to version 17.0.0, an unprotected intend allowed malicious third party apps to trick the Talk Android app into writing files outside of its intended cache directory. Nextcloud Talk Android version 17.0.0 has a patch for this issue. No known workarounds are available.	7.8	More Details
CVE-2023-3160	The vulnerability potentially allows an attacker to misuse ESET's file operations during the module update to delete or move files without having proper permissions.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40303	GNU inetutils before 2.5 may allow privilege escalation because of unchecked return values of set*id() family functions in ftpd, rcp, rlogin, rsh, rshd, and uucpd. This is, for example, relevant if the setuid system call fails when a process is trying to drop privileges before letting an ordinary user control the activities of the process.	7.8	More Details
CVE-2023-28129	DSM 2022.2 SU2 and all prior versions allows a local low privileged account to execute arbitrary OS commands as the DSM software installation user.	7.8	More Details
CVE-2023-40283	An issue was discovered in l2cap_sock_release in net/bluetooth/l2cap_sock.c in the Linux kernel before 6.4.10. There is a use-after-free because the children of an sk are mishandled.	7.8	More Details
CVE-2023-26587	Improper input validation for the Intel(R) Easy Streaming Wizard software may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2023-22955	An issue was discovered on AudioCodes VoIP desk phones through 3.4.4.1000. The validation of firmware images only consists of simple checksum checks for different firmware components. Thus, by knowing how to calculate and where to store the required checksums for the flasher tool, an attacker is able to store malicious firmware.	7.8	More Details
CVE-2023-21235	In onCreate of LockSettingsActivity.java, there is a possible way set a new lockscreen PIN without entering the existing PIN 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.	7.8	More Details
CVE-2021-28835	Buffer Overflow vulnerability in XNView before 2.50, allows local attackers to execute arbitrary code via crafted GEM bitmap file.	7.8	More Details
CVE-2021-28427	Buffer Overflow vulnerability in XNView version 2.49.3, allows local attackers to execute arbitrary code via crafted TIFF file.	7.8	More Details
CVE-2020-28840	Buffer Overflow vulnerability in jpgfile.c in Matthias-Wandel jhead version 3.04, allows local attackers to execute arbitrary code and cause a denial of service (DoS).	7.8	More Details
CVE-2023-21231	In getIntentForButton of ButtonManager.java, there is a possible way for an unprivileged application to start a non-exported or permission-protected activity due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24222	Buffer Overflow vulnerability in jfif_decode() function in rockcarry ffjpeg through version 1.0.0, allows local attackers to execute arbitrary code due to an issue with ALIGN.	7.8	More Details
CVE-2020-36615	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1. Processing a maliciously crafted font may lead to arbitrary code execution.	7.8	More Details
CVE-2023-33469	In instances where the screen is visible and remote mouse connection is enabled, KramerAV VIA Connect (2) and VIA Go (2) devices with a version prior to 4.0.1.1326 can be exploited to achieve local code execution at the root level.	7.8	More Details
CVE-2023-38212	Adobe Dimension version 3.4.9 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-2023-30679	Improper access control in HDCP trustlet prior to SMR Aug-2023 Release 1 allows local attackers to execute arbitrary code.	7.8	More Details
CVE-2023-38211	Adobe Dimension version 3.4.9 is affected by a Use After Free 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-2023-21286	In visitUris of RemoteViews.java, there is a possible way to reveal images across users due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2022-46706	A type confusion issue was addressed with improved state handling. This issue is fixed in Security Update 2022-003 Catalina, macOS Monterey 12.3, macOS Big Sur 11.6.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-38401	A vulnerability in the HPE Aruba Networking Virtual Intranet Access (VIA) client could allow local users to elevate privileges. Successful exploitation could allow execution of arbitrary code with NT AUTHORITY\SYSTEM privileges on the operating system.	7.8	More Details
CVE-2023-21275	In decideCancelProvisioningDialog of AdminIntegratedFlowPrepareActivity.java, there is a possible way to bypass factory reset protections due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21272	In readFrom of Uri.java, there is a possible bad URI permission grant due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-35689	In checkDebuggingDisallowed of DeviceVersionFragment.java, there is a possible way to access adb before SUW completion due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-21281	In multiple functions of KeyguardViewMediator.java, there is a possible failure to lock after screen timeout due to a logic error in the code. This could lead to local escalation of privilege across users with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-39962	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 19.0.0 and prior to versions 19.0.13.10, 20.0.14.15, 21.0.9.13, 22.2.10.14, 23.0.12.8, 24.0.12.5, 25.0.9, 26.0.4, and 27.0.1, a malicious user could delete any personal or global external storage, making them inaccessible for everyone else as well. Nextcloud server versions 25.0.9, 26.0.4, and 27.0.1 and Nextcloud Enterprise Server versions 19.0.13.10, 20.0.14.15, 21.0.9.13, 22.2.10.14, 23.0.12.9, 24.0.12.5, 25.0.9, 26.0.4, and 27.0.1 contain a patch for this issue. As a workaround, disable app files_external. This also makes the external storage inaccessible but retains the configurations until a patched version has been deployed.	7.7	More Details
CVE-2023-39389	Vulnerability of input parameters being not strictly verified in the PMS module. Successful exploitation of this vulnerability may cause home screen unavailability.	7.5	More Details
CVE-2023-40296	async-sockets-cpp through 0.3.1 has a stack-based buffer overflow in ReceiveFrom and Receive in udpsocket.hpp when processing malformed UDP packets.	7.5	More Details
CVE-2023-39392	Vulnerability of insecure signatures in the OsuLogin module. Successful exploitation of this vulnerability may cause OsuLogin to be maliciously modified and overwritten.	7.5	More Details
CVE-2023-3263	The Dataprobe iBoot PDU running firmware version 1.43.03312023 or earlier is vulnerable to authentication bypass in the REST API due to the mishandling of special characters when parsing credentials.Successful exploitation allows the malicious agent to obtain a valid authorization token and read information relating to the state of the relays and power distribution.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39394	Vulnerability of API privilege escalation in the wifienhance module. Successful exploitation of this vulnerability may cause the arp list to be modified.	7.5	More Details
CVE-2023-39393	Vulnerability of insecure signatures in the ServiceWifiResources module. Successful exploitation of this vulnerability may cause ServiceWifiResources to be maliciously modified and overwritten.	7.5	More Details
CVE-2023-30188	Memory Exhaustion vulnerability in ONLYOFFICE Document Server 4.0.3 through 7.3.2 allows remote attackers to cause a denial of service via crafted JavaScript file.	7.5	More Details
CVE-2023-39384	Vulnerability of incomplete permission verification in the input method module. Successful exploitation of this vulnerability may cause features to perform abnormally.	7.5	More Details
CVE-2023-39383	Vulnerability of input parameters being not strictly verified in the AMS module. Successful exploitation of this vulnerability may compromise apps' data security.	7.5	More Details
CVE-2023-39382	Input verification vulnerability in the audio module. Successful exploitation of this vulnerability may cause virtual machines (VMs) to restart.	7.5	More Details
CVE-2023-39381	Input verification vulnerability in the storage module. Successful exploitation of this vulnerability may cause the device to restart.	7.5	More Details
CVE-2023-22449	Improper input validation in 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-2023-38830	An information leak in PHPJabbers Yacht Listing Script v1.0 allows attackers to export clients' credit card numbers from the Reservations module.	7.5	More Details
CVE-2023-39388	Vulnerability of input parameters being not strictly verified in the PMS module. Successful exploitation of this vulnerability may cause home screen unavailability.	7.5	More Details
CVE-2023-39003	OPNsense Community Edition before 23.7 and Business Edition before 23.4.2 was discovered to contain insecure permissions in the directory /tmp.	7.5	More Details
CVE-2023-39396	Deserialization vulnerability in the input module. Successful exploitation of this vulnerability may affect availability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36372	Improper buffer restrictions in 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-2023-4339	Broadcom RAID Controller web interface is vulnerable to exposure of private keys used for CIM stored with insecure file permissions	7.5	More Details
CVE-2023-4343	Broadcom RAID Controller web interface is vulnerable due to exposure of sensitive password information in the URL as a URL search parameter	7.5	More Details
CVE-2023-39404	Vulnerability of input parameter verification in certain APIs in the window management module. Successful exploitation of this vulnerability may cause the device to restart.	7.5	More Details
CVE-2023-39406	Permission control vulnerability in the XLayout component. Successful exploitation of this vulnerability may cause apps to forcibly restart.	7.5	More Details
CVE-2023-40274	An issue was discovered in zola 0.13.0 through 0.17.2. The custom implementation of a web server, available via the "zola serve" command, allows directory traversal. The handle_request function, used by the server to process HTTP requests, does not account for sequences of special path control characters (../) in the URL when serving a file, which allows one to escape the webroot of the server and read arbitrary files from the filesystem.	7.5	More Details
CVE-2023-39391	Vulnerability of system file information leakage in the USB Service module. Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details
CVE-2023-2916	The InfiniteWP Client plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 1.11.1 via the 'admin_notice' function. This can allow authenticated attackers with subscriber-level permissions or above to extract sensitive data including configuration. It can only be exploited if the plugin has not been configured yet. If combined with another arbitrary plugin installation and activation vulnerability, it may be possible to connect a site to InfiniteWP which would make remote management possible and allow for elevation of privileges.	7.5	More Details
CVE-2023-3261	The Dataprobe iBoot PDU running firmware version 1.43.03312023 or earlier contains a buffer overflow vulnerability in the librta.so.0.0.0 library.Successful exploitation could cause denial of service or unexpected behavior with respect to all interactions relying on the targeted vulnerable binary, including the ability to log in via the web server.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4334	Broadcom RAID Controller Web server (nginx) is serving private files without any authentication	7.5	More Details
CVE-2023-39005	Insecure permissions exist for configd.socket in OPNsense Community Edition before 23.7 and Business Edition before 23.4.2.	7.5	More Details
CVE-2023-32561	A previously generated artifact by an administrator could be accessed by an attacker. The contents of this artifact could lead to authentication bypass. Fixed in version 6.4.1.	7.5	More Details
CVE-2023-39390	Vulnerability of input parameter verification in certain APIs in the window management module. Successful exploitation of this vulnerability may cause the device to restart.	7.5	More Details
CVE-2023-39386	Vulnerability of input parameters being not strictly verified in the PMS module. Successful exploitation of this vulnerability may cause newly installed apps to fail to restart.	7.5	More Details
CVE-2023-39966	1Panel is an open source Linux server operation and maintenance management panel. In version 1.4.3, an arbitrary file write vulnerability could lead to direct control of the server. In the `api/v1/file.go` file, there is a function called `SaveContentthat,It `recieves JSON data sent by users in the form of a POST request. And the lack of parameter filtering allows for arbitrary file write operations. Version 1.5.0 contains a patch for this issue.	7.5	More Details
CVE-2023-4335	Broadcom RAID Controller Web server (nginx) is serving private server-side files without any authentication on Linux	7.5	More Details
CVE-2023-39964	1Panel is an open source Linux server operation and maintenance management panel. In version 1.4.3, arbitrary file reads allow an attacker to read arbitrary important configuration files on the server. In the `api/v1/file.go` file, there is a function called `LoadFromFile`, which directly reads the file by obtaining the requested path `parameter[path]`. The request parameters are not filtered, resulting in a background arbitrary file reading vulnerability. Version 1.5.0 has a patch for this issue.	7.5	More Details
CVE-2023-37543	Cacti before 1.2.6 allows IDOR (Insecure Direct Object Reference) for accessing any graph via a modified local_graph_id parameter to graph_xport.php. This is a different vulnerability than CVE-2019-16723.	7.5	More Details
CVE-2023-22956	An issue was discovered on AudioCodes VoIP desk phones through 3.4.4.1000. Due to the use of a hard-coded cryptographic key, an attacker is able to decrypt encrypted configuration files and retrieve sensitive information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31041	An issue was discovered in SysPasswordDxe in Insyde InsydeH2O with kernel 5.0 through 5.5. System password information could optionally be stored in cleartext, which might lead to possible information disclosure.	7.5	More Details
CVE-2023-39380	Permission control vulnerability in the audio module. Successful exploitation of this vulnerability may cause audio devices to perform abnormally.	7.5	More Details
CVE-2023-40254	Download of Code Without Integrity Check vulnerability in Genians Genian NAC V4.0, Genians Genian NAC V5.0, Genians Genian NAC Suite V5.0, Genians Genian ZTNA allows Malicious Software Update.This issue affects Genian NAC V4.0: from V4.0.0 through V4.0.155; Genian NAC V5.0: from V5.0.0 through V5.0.42 (Revision 117460); Genian NAC Suite V5.0: from V5.0.0 through V5.0.54; Genian ZTNA: from V6.0.0 through V6.0.15.	7.5	More Details
CVE-2023-4331	Broadcom RAID Controller web interface is vulnerable has an insecure default TLS configuration that support obsolete and vulnerable TLS protocols	7.5	More Details
CVE-2020-36136	SQL Injection vulnerability in cskaza cszcms version 1.2.9, allows attackers to gain sensitive information via pm_sendmail parameter in csz_model.php.	7.5	More Details
CVE-2023-39553	Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow Drill Provider. Apache Airflow Drill Provider is affected by a vulnerability that allows an attacker to pass in malicious parameters when establishing a connection with DrillHook giving an opportunity to read files on the Airflow server. This issue affects Apache Airflow Drill Provider: before 2.4.3. It is recommended to upgrade to a version that is not affected.	7.5	More Details
CVE-2020-35141	An issue was discovered in OFPQueueGetConfigReply in parser.py in Faucet SDN Ryu version 4.34, allows remote attackers to cause a denial of service (DoS) (infinite loop).	7.5	More Details
CVE-2023-21265	In multiple locations, there are root CA certificates which need to be disabled. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2023-39417	IN THE EXTENSION SCRIPT, a SQL Injection vulnerability was found in PostgreSQL if it uses @extowner@, @extschema@, or @extschema:...@ inside a quoting construct (dollar quoting, '', or ""). If an administrator has installed files of a vulnerable, trusted, non-bundled extension, an attacker with database-level CREATE privilege can execute arbitrary code as the bootstrap superuser.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35139	An issue was discovered in OFPBundleCtrlMsg in parser.py in Faucet SDN Ryu version 4.34, allows remote attackers to cause a denial of service (DoS) (infinite loop).	7.5	More Details
CVE-2023-37860	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon.	7.5	More Details
CVE-2023-39827	Tenda A18 V15.13.07.09 was discovered to contain a stack overflow via the rule_info parameter in the formAddMacfilterRule function.	7.5	More Details
CVE-2023-39828	Tenda A18 V15.13.07.09 was discovered to contain a stack overflow via the security parameter in the formWifiBasicSet function.	7.5	More Details
CVE-2023-39829	Tenda A18 V15.13.07.09 was discovered to contain a stack overflow via the wpapsk_crypto2_4g parameter in the fromSetWirelessRepeat function.	7.5	More Details
CVE-2023-4326	Broadcom RAID Controller web interface is vulnerable has an insecure default TLS configuration that supports obsolete SHA1-based ciphersuites	7.5	More Details
CVE-2022-47185	Improper input validation vulnerability on the range header in Apache Software Foundation Apache Traffic Server.This issue affects Apache Traffic Server: through 9.2.1.	7.5	More Details
CVE-2023-21233	In multiple locations of avrc, there is a possible leak of heap data due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2020-36138	An issue was discovered in decode_frame in libavcodec/tiff.c in FFmpeg version 4.3, allows remote attackers to cause a denial of service (DoS).	7.5	More Details
CVE-2023-34438	Race condition in 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-2023-40518	LiteSpeed OpenLiteSpeed before 1.7.18 does not strictly validate HTTP request headers.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30699	Out-of-bounds write vulnerability in parser_hvcC function of libsimba library prior to SMR Aug-2023 Release 1 allows code execution by remote attackers.	7.5	More Details
CVE-2023-25773	Improper access control in the Intel(R) Unite(R) Hub software installer for Windows before version 4.2.34962 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2023-22957	An issue was discovered in libac_des3.so on AudioCodes VoIP desk phones through 3.4.4.1000. Due to the use of hard-coded cryptographic key, an attacker with access to backup or configuration files is able to decrypt encrypted values and retrieve sensitive information, e.g., the device root password.	7.5	More Details
CVE-2023-39395	Mismatch vulnerability in the serialization process in the communication system. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2023-39949	eprosima Fast DDS is a C++ implementation of the Data Distribution Service standard of the Object Management Group. Prior to versions 2.9.1 and 2.6.5, improper validation of sequence numbers may lead to remotely reachable assertion failure. This can remotely crash any Fast-DDS process. Versions 2.9.1 and 2.6.5 contain a patch for this issue.	7.5	More Details
CVE-2023-38741	IBM TXSeries for Multiplatforms 8.1, 8.2, and 9.1 is vulnerable to a denial of service, caused by improper enforcement of the timeout on individual read operations. By conducting a slowloris-type attacks, a remote attacker could exploit this vulnerability to cause a denial of service. IBM X-Force ID: 262905.	7.5	More Details
CVE-2023-39948	eprosima Fast DDS is a C++ implementation of the Data Distribution Service standard of the Object Management Group. Prior to versions 2.10.0 and 2.6.5, the `BadParamException` thrown by Fast CDR is not caught in Fast DDS. This can remotely crash any Fast DDS process. Versions 2.10.0 and 2.6.5 contain a patch for this issue.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33953	gRPC contains a vulnerability that allows hpack table accounting errors could lead to unwanted disconnects between clients and servers in exceptional cases/ Three vectors were found that allow the following DOS attacks: - Unbounded memory buffering in the HPACK parser - Unbounded CPU consumption in the HPACK parser The unbounded CPU consumption is down to a copy that occurred per-input-block in the parser, and because that could be unbounded due to the memory copy bug we end up with an O(n^2) parsing loop, with n selected by the client. The unbounded memory buffering bugs: - The header size limit check was behind the string reading code, so we needed to first buffer up to a 4 gigabyte string before rejecting it as longer than 8 or 16kb. - HPACK varints have an encoding quirk whereby an infinite number of 0's can be added at the start of an integer. gRPC's hpack parser needed to read all of them before concluding a parse. - gRPC's metadata overflow check was performed per frame, so that the following sequence of frames could cause infinite buffering: HEADERS: containing a: 1 CONTINUATION: containing a: 2 CONTINUATION: containing a: 3 etc…	7.5	More Details
CVE-2023-29494	Improper input validation in BIOS firmware for some Intel(R) NUCs may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2023-39534	eprosima Fast DDS is a C++ implementation of the Data Distribution Service standard of the Object Management Group. Prior to versions 2.10.0, 2.9.2, and 2.6.5, a malformed GAP submessage can trigger assertion failure, crashing FastDDS. Version 2.10.0, 2.9.2, and 2.6.5 contain a patch for this issue.	7.5	More Details
CVE-2023-39910	The cryptocurrency wallet entropy seeding mechanism used in Libbitcoin Explorer 3.0.0 through 3.6.0 is weak, aka the Milk Sad issue. The use of an mt19937 Mersenne Twister PRNG restricts the internal entropy to 32 bits regardless of settings. This allows remote attackers to recover any wallet private keys generated from "bx seed" entropy output and steal funds. (Affected users need to move funds to a secure new cryptocurrency wallet.) NOTE: the vendor's position is that there was sufficient documentation advising against "bx seed" but others disagree. NOTE: this was exploited in the wild in June and July 2023.	7.5	More Details
CVE-2023-39908	The PKCS11 module of the YubiHSM 2 SDK through 2023.01 does not properly validate the length of specific read operations on object metadata. This may lead to disclosure of uninitialized and previously used memory.	7.5	More Details
CVE-2023-4332	Broadcom RAID Controller web interface is vulnerable due to Improper permissions on the log file	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38207	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by a XML Injection (aka Blind XPath Injection) vulnerability that could lead in minor arbitrary file system read. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2021-26504	Directory Traversal vulnerability in Foddy node-red-contrib-huemagic version 3.0.0, allows remote attackers to gain sensitive information via crafted request in res.sendFile API in hue-magic.js.	7.5	More Details
CVE-2023-39397	Input parameter verification vulnerability in the communication system. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2023-3518	HashiCorp Consul and Consul Enterprise 1.16.0 when using JWT Auth for service mesh incorrectly allows/denies access regardless of service identities. Fixed in 1.16.1.	7.4	More Details
CVE-2023-26310	There is a command injection problem in the old version of the mobile phone backup app.	7.4	More Details
CVE-2023-26311	A remote code execution vulnerability in the webview component of OPPO Store app.	7.4	More Details
CVE-2023-26309	A remote code execution vulnerability in the webview component of OnePlus Store app.	7.4	More Details
CVE-2023-25757	Improper access control in some Intel(R) Unison(TM) software before version 10.12 may allow a privileged user to potentially enable escalation of privilege via network access.	7.3	More Details
CVE-2022-45112	Improper access control in some Intel(R) VROC software before version 8.0.0.4035 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.3	More Details
CVE-2023-36673	An issue was discovered in Avira Phantom VPN through 2.23.1 for macOS. The VPN client insecurely configures the operating system such that all IP traffic to the VPN server's IP address is sent in plaintext outside the VPN tunnel, even if this traffic is not generated by the VPN client, while simultaneously using plaintext DNS to look up the VPN server's IP address. This allows an adversary to trick the victim into sending traffic to arbitrary IP addresses in plaintext outside the VPN tunnel. NOTE: the tunnelcrack.mathyvanhoef.com website uses this CVE ID to refer more generally to "ServerIP attack, combined with DNS spoofing, that can leak traffic to an arbitrary IP address" rather than to only Avira Phantom VPN.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37343	Improper access control in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	More Details
CVE-2023-37863	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device.	7.2	More Details
CVE-2022-41804	Unauthorized error injection in Intel(R) SGX or Intel(R) TDX for some Intel(R) Xeon(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	More Details
CVE-2023-37864	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device.	7.2	More Details
CVE-2022-38102	Improper Input validation in firmware for some Intel(R) Converged Security and Management Engine before versions 15.0.45, and 16.1.27 may allow a privileged user to potentially enable denial of service via local access.	7.2	More Details
CVE-2023-4308	The User Submitted Posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘user-submitted-content’ parameter in versions up to, and including, 20230809 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2023-3864	Blind SQL injection in a service running in Snow Software license manager from version 8.0.0 up to and including 9.30.1 on Windows allows a logged in user with high privileges to inject SQL commands via the web portal.	7.2	More Details
CVE-2023-37859	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP daemon is running with root privileges allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root.	7.2	More Details
CVE-2023-38997	A directory traversal vulnerability in the Captive Portal templates of OPNsense Community Edition before 23.7 and Business Edition before 23.4.2 allows attackers to execute arbitrary system commands as root via a crafted ZIP archive.	7.2	More Details
CVE-2023-3260	The Dataprobe iBoot PDU running firmware version 1.43.03312023 or earlier is vulnerable to command injection via the `user-name` URL parameter. An authenticated malicious agent can exploit this vulnerability to execute arbitrary command on the underlying Linux operating system.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40225	HAProxy through 2.0.32, 2.1.x and 2.2.x through 2.2.30, 2.3.x and 2.4.x through 2.4.23, 2.5.x and 2.6.x before 2.6.15, 2.7.x before 2.7.10, and 2.8.x before 2.8.2 forwards empty Content-Length headers, violating RFC 9110 section 8.6. In uncommon cases, an HTTP/1 server behind HAProxy may interpret the payload as an extra request.	7.2	More Details
CVE-2021-25857	An issue was discovered in pcmt superMicro-CMS version 3.11, allows authenticated attackers to execute arbitrary code via the font_type parameter to setup.php.	7.2	More Details
CVE-2023-35179	A vulnerability has been identified within Serv-U 15.4 that, if exploited, allows an actor to bypass multi-factor/two-factor authentication. The actor must have administrator-level access to Serv-U to perform this action.	7.2	More Details
CVE-2023-32781	A command injection vulnerability was identified in PRTG 23.2.84.1566 and earlier versions in the HL7 sensor where an authenticated user with write permissions could abuse the debug option to write new files that could potentially get executed by the EXE/Script sensor. The severity of this vulnerability is high and received a score of 7.2 CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2	More Details
CVE-2023-32782	A command injection was identified in PRTG 23.2.84.1566 and earlier versions in the Dicom C-ECHO sensor where an authenticated user with write permissions could abuse the debug option to write new files that could potentially get executed by the EXE/Script sensor. The severity of this vulnerability is high and received a score of 7.2 CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2	More Details
CVE-2023-28179	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. Processing a maliciously crafted AppleScript binary may result in unexpected app termination or disclosure of process memory.	7.1	More Details
CVE-2023-30754	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in AdFoxly AdFoxly – Ad Manager, AdSense Ads & Ads.Txt plugin <= 1.8.5 versions.	7.1	More Details
CVE-2023-30489	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution Email Subscription Popup plugin <= 1.2.16 versions.	7.1	More Details
CVE-2023-28535	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Paytm Paytm Payment Donation plugin <= 2.2.0 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30475	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Elliot Sowersby, RelyWP WooCommerce Affiliate Plugin – Coupon Affiliates plugin <= 5.4.5 versions.	7.1	More Details
CVE-2023-30498	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in CodeFlavors Vimeotheque: Vimeo WordPress Plugin <= 2.2.1 versions.	7.1	More Details
CVE-2023-30483	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Kiboko Labs Watu Quiz plugin <= 3.3.9.2 versions.	7.1	More Details
CVE-2023-37988	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Creative Solutions Contact Form Generator plugin <= 2.5.5 versions.	7.1	More Details
CVE-2023-28779	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Vladimir Statsenko Terms descriptions plugin <= 3.4.4 versions.	7.1	More Details
CVE-2023-30747	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WPGem WooCommerce Easy Duplicate Product plugin <= 0.3.0.0 versions.	7.1	More Details
CVE-2023-39314	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Teplitsa of social technologies Leyka plugin <= 3.30.2 versions.	7.1	More Details
CVE-2023-38402	A vulnerability in the HPE Aruba Networking Virtual Intranet Access (VIA) client could allow malicious users to overwrite arbitrary files as NT AUTHORITY\SYSTEM. A successful exploit could allow these malicious users to create a Denial-of-Service (DoS) condition affecting the Microsoft Windows operating System boot process.	7.1	More Details
CVE-2023-30481	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Alexey Golubnichenko AGP Font Awesome Collection plugin <= 3.2.4 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40013	SVG Loader is a javascript library that fetches SVGs using XMLHttpRequests and injects the SVG code in the tag's place. According to the docs, svg-loader will strip all JS code before injecting the SVG file for security reasons but the input sanitization logic is not sufficient and can be trivially bypassed. This allows an attacker to craft a malicious SVG which can result in Cross-site Scripting (XSS). When trying to sanitize the svg the lib removes event attributes such as `onmouseover`, `onclick` but the list of events is not exhaustive. Any website which uses external-svg-loader and allows its users to provide svg src, upload svg files would be susceptible to stored XSS attack. This issue has been addressed in commit `d3562fc08` which is included in releases from 1.6.9. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.1	More Details
CVE-2023-24477	In certain conditions, depending on timing and the usage of the Chrome web browser, Guardian/CMC versions before 22.6.2 do not always completely invalidate the user session upon logout. Thus an authenticated local attacker may gain acces to the original user's session.	7.0	More Details
CVE-2022-44611	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via adjacent access.	6.9	More Details
CVE-2023-21133	In onCreate of ManagePermissionsActivity.java, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.	6.8	More Details
CVE-2023-30705	Improper sanitization of incoming intent in Galaxy Store prior to version 4.5.56.6?allows local attackers to access privileged content providers as Galaxy Store permission.	6.8	More Details
CVE-2023-21132	In onCreate of ManagePermissionsActivity.java, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.	6.8	More Details
CVE-2023-40291	Harman Infotainment 20190525031613 allows root access via SSH over a USB-to-Ethernet dongle with a password that is an internal project name.	6.8	More Details
CVE-2023-40293	Harman Infotainment 20190525031613 and later allows command injection via unauthenticated RPC with a D-Bus connection object.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21140	In onCreate of ManagePermissionsActivity.java, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.	6.8	More Details
CVE-2023-21134	In onCreate of ManagePermissionsActivity.java, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.	6.8	More Details
CVE-2023-31246	Incorrect default permissions in some Intel(R) SDP Tool software before version 1.4 build 5 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-21264	In multiple functions of mem_protect.c, there is a possible way to access hypervisor memory due to a memory access check in the wrong place. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2023-30694	Out-of-bounds Write in IpcTxPcscTransmitApdu of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2023-32547	Incorrect default permissions in the MAVinci Desktop Software for Intel(R) Falcon 8+ before version 6.2 may allow authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-32543	Incorrect default permissions in the Intel(R) ITS sofware before version 3.1 may allow authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-30702	Stack overflow vulnerability in SSHDCPAPP TA prior to "SAMSUNG ELECTONICS, CO, LTD. - System Hardware Update - 7/13/2023" in Windows Update for Galaxy book Go, Galaxy book Go 5G, Galaxy book2 Go and Galaxy book2 Pro 360 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2023-30695	Out-of-bounds Write vulnerability in SSHDCPAPP TA prior to "SAMSUNG ELECTONICS, CO, LTD. - System Hardware Update - 7/13/2023" in Windows Update for Galaxy book Go, Galaxy book Go 5G, Galaxy book2 Go and Galaxy book2 Pro 360 allows local attacker to execute arbitrary code.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32663	Incorrect default permissions in some Intel(R) RealSense(TM) SDKs in version 2.53.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-34355	Uncontrolled search path element for some Intel(R) Server Board M10JNP2SB integrated BMC video drivers before version 3.0 for Microsoft Windows and before version 1.13.4 for linux may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-28823	Uncontrolled search path in some Intel(R) oneAPI Toolkit and component software installers before version 4.3.1.493 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-20564	Insufficient validation in the IOCTL (Input Output Control) input buffer in AMD Ryzen™ Master may permit a privileged attacker to perform memory reads/writes potentially leading to a loss of confidentiality or arbitrary kernel execution.	6.7	More Details
CVE-2023-4107	Mattermost fails to properly validate the requesting user permissions when updating a system admin, allowing a user manager to update a system admin's details such as email, first name and last name.	6.7	More Details
CVE-2023-40312	Multiple reflected XSS were found on different JSP files with unsanitized parameters in OpenMNS Horizon 31.0.8 and versions earlier than 32.0.2 on multiple platforms that an attacker can modify to craft a malicious XSS payload. The solution is to upgrade to Meridian 2023.1.6, 2022.1.19, 2021.1.30, 2020.1.38 or Horizon 32.0.2 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. OpenNMS thanks Jordi Miralles Comins for reporting this issue.	6.7	More Details
CVE-2023-29151	Uncontrolled search path element in some Intel(R) PSR SDK before version 1.0.0.20 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-25944	Uncontrolled search path element in some Intel(R) VCUST Tool software downloaded before February 3nd 2023 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-23577	Uncontrolled search path element for some ITE Tech consumer infrared drivers before version 5.5.2.1 for Intel(R) NUC may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-24016	Uncontrolled search path element in some Intel(R) Quartus(R) Prime Pro and Standard edition software for linux 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-2023-30686	Out-of-bounds Write in ReqDataRaw of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2023-30687	Out-of-bounds Write in RmtUimApdu of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2023-27391	Improper access control in some Intel(R) oneAPI Toolkit and component software installers before version 4.3.1.493 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-30688	Out-of-bounds Write in MakeUiccAuthForOem of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2023-27505	Incorrect default permissions in some Intel(R) Advanced Link Analyzer Standard Edition software installers before version 22.1 .1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-3264	The Dataprobe iBoot PDU running firmware version 1.43.03312023 or earlier uses hard-coded credentials for all interactions with the internal Postgres database. A malicious agent with the ability to execute operating system commands on the device can leverage this vulnerability to read, modify, or delete arbitrary database records.	6.7	More Details
CVE-2023-30654	Improper access control vulnerability in SLocationService prior to SMR Aug-2023 Release 1 allows local attacker to update fake location.	6.7	More Details
CVE-2022-43456	Uncontrolled search path in some Intel(R) RST software before versions 16.8.5.1014.5, 17.11.3.1010.2, 18.7.6.1011.2 and 19.5.2.1049.5 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-22841	Unquoted search path in the software installer for the System Firmware Update Utility (SysFwUpdt) for some Intel(R) Server Boards and Intel(R) Server Systems Based on Intel(R) 621A Chipset before version 16.0.7 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-3262	The Dataprobe iBoot PDU running firmware version 1.43.03312023 or earlier uses hard-coded credentials for all interactions with the internal Postgres database.A malicious agent with the ability to execute operating system commands on the device can leverage this vulnerability to read, modify, or delete arbitrary database records.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30689	Out-of-bounds Write in BuildOemEmbmsGetSigStrengthResponse of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2022-25864	Uncontrolled search path in some Intel(R) oneMKL software before version 2022.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-29871	Improper access control in the Intel(R) CSME software installer before version 2239.3.7.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-30693	Out-of-bounds Write in DoOemFactorySendFactoryBypassCommand of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2022-29470	Improper access control in the Intel® DTT Software before version 8.7.10400.15482 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-28405	Uncontrolled search path in the Intel(R) Distribution of OpenVINO(TM) Toolkit before version 2022.3.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-28658	Insecure inherited permissions in some Intel(R) oneMKL software before version 2022.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-40311	Multiple stored XSS were found on different JSP files with unsanitized parameters in OpenMNS Horizon 31.0.8 and versions earlier than 32.0.2 on multiple platforms that allow an attacker to store on database and then load on JSPs or Angular templates. The solution is to upgrade to Meridian 2023.1.6, 2022.1.19, 2021.1.30, 2020.1.38 or Horizon 32.0.2 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. OpenNMS thanks Jordi Miralles Comins for reporting this issue.	6.7	More Details
CVE-2023-23342	If certain local files are manipulated in a certain manner, the validation to use the cryptographic keys can be circumvented.	6.6	More Details
CVE-2023-27509	Improper access control in some Intel(R) ISPC software installers before version 1.19.0 may allow an authenticated user to potentially enable escalation of privileges via local access.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36023	An issue was discovered in freedesktop poppler version 20.12.1, allows remote attackers to cause a denial of service (DoS) via crafted .pdf file to FoFiType1C::cvtGlyph function.	6.5	More Details
CVE-2023-38851	Buffer Overflow vulnerability in libxlsv.1.6.2 allows a remote attacker to execute arbitrary code and cause a denial of service via a crafted XLS file to the xls_parseWorkBook function in xls.c:1018.	6.5	More Details
CVE-2020-24904	An issue was discovered in attach parameter in GNOME Gmail version 2.5.4, allows remote attackers to gain sensitive information via crafted "mailto" link.	6.5	More Details
CVE-2023-40294	libboron in Boron 2.0.8 has a heap-based buffer overflow in ur_parseBlockI at i_parse_blk.c.	6.5	More Details
CVE-2023-38858	Buffer Overflow vulnerability infaad2 v.2.10.1 allows a remote attacker to execute arbitrary code and cause a denial of service via the mp4info function in mp4read.c:1039.	6.5	More Details
CVE-2023-28768	Improper frame handling in the Zyxel XGS2220-30 firmware version V4.80(ABXN.1), XMG1930-30 firmware version V4.80(ACAR.1), and XS1930-10 firmware version V4.80(ABQE.1) could allow an unauthenticated LAN-based attacker to cause denial-of-service (DoS) conditions by sending crafted frames to an affected switch.	6.5	More Details
CVE-2023-38852	Buffer Overflow vulnerability in libxlsv.1.6.2 allows a remote attacker to execute arbitrary code and cause a denial of service via a crafted XLS file to the unicode_decode_wcstombs function in xlstool.c:266.	6.5	More Details
CVE-2023-40354	An issue was discovered in MariaDB MaxScale before 23.02.3. A user enters an encrypted password on a "maxctrl create service" command line, but this password is then stored in cleartext in the resulting .cnf file under /var/lib/maxscale/maxscale.cnf.d. The fixed versions are 2.5.28, 6.4.9, 22.08.8, and 23.02.3.	6.5	More Details
CVE-2023-38856	Buffer Overflow vulnerability in libxlsv.1.6.2 allows a remote attacker to execute arbitrary code and cause a denial of service via a crafted XLS file to the get_string function in xlstool.c:411.	6.5	More Details
CVE-2023-38853	Buffer Overflow vulnerability in libxlsv.1.6.2 allows a remote attacker to execute arbitrary code and cause a denial of service via a crafted XLS file to the xls_parseWorkBook function in xls.c:1015.	6.5	More Details
CVE-2020-24804	Plaintext Password vulnerability in AddAdmin.py in cms-dev/cms v1.4.rc1, allows attackers to gain sensitive information via audit logs.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40023	yaklang is a programming language designed for cybersecurity. The Yak Engine has been found to contain a local file inclusion (LFI) vulnerability. This vulnerability allows attackers to include files from the server's local file system through the web application. When exploited, this can lead to the unintended exposure of sensitive data, potential remote code execution, or other security breaches. Users utilizing versions of the Yak Engine prior to 1.2.4-sp1 are impacted. This vulnerability has been patched in version 1.2.4-sp1. Users are advised to upgrade. users unable to upgrade may avoid exposing vulnerable versions to untrusted input and to closely monitor any unexpected server behavior until they can upgrade.	6.5	More Details
CVE-2023-38854	Buffer Overflow vulnerability in libxlsv.1.6.2 allows a remote attacker to execute arbitrary code and cause a denial of service via a crafted XLS file to the transcode_latin1_to_utf8 function in xlstool.c:296.	6.5	More Details
CVE-2023-28482	An issue was discovered in Tigergraph Enterprise 3.7.0. A single TigerGraph instance can host multiple graphs that are accessed by multiple different users. The TigerGraph platform does not protect the confidentiality of any data uploaded to the remote server. In this scenario, any user that has permissions to upload data can browse data uploaded by any other user (irrespective of their permissions).	6.5	More Details
CVE-2023-4350	Inappropriate implementation in Fullscreen in Google Chrome on Android prior to 116.0.5845.96 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2021-29057	An issue was discovered in StaticPool in SUCHMOKUO node-worker-threads-pool version 1.4.3, allows attackers to cause a denial of service.	6.5	More Details
CVE-2023-4345	Broadcom RAID Controller web interface is vulnerable client-side control bypass leads to unauthorized data access for low privileged user	6.5	More Details
CVE-2023-28480	An issue was discovered in Tigergraph Enterprise 3.7.0. The TigerGraph platform allows users to define new User Defined Functions (UDFs) from C/C++ code. To support this functionality TigerGraph allows users to upload custom C/C++ code which is then compiled and installed into the platform. An attacker who has filesystem access on a remote TigerGraph system can alter the behavior of the database against the will of the database administrator; thus effectively bypassing the built in RBAC controls.	6.5	More Details
CVE-2023-38855	Buffer Overflow vulnerability in libxlsv.1.6.2 allows a remote attacker to execute arbitrary code and cause a denial of service via a crafted XLS file to the get_string function in xlstool.c:395.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4367	Insufficient policy enforcement in Extensions API in Google Chrome prior to 116.0.5845.96 allowed an attacker who convinced a user to install a malicious extension to bypass an enterprise policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2022-40982	Information exposure through microarchitectural state after transient execution in certain vector execution units for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	6.5	More Details
CVE-2023-37983	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Noël Jackson Art Direction plugin <= 0.2.4 versions.	6.5	More Details
CVE-2023-22276	Race condition in firmware for some Intel(R) Ethernet Controllers and Adapters E810 Series before version 1.7.2.4 may allow an authenticated user to potentially enable denial of service via local access.	6.5	More Details
CVE-2023-38999	A Cross-Site Request Forgery (CSRF) in the System Halt API (/system/halt) of OPNsense Community Edition before 23.7 and Business Edition before 23.4.2 allows attackers to cause a Denial of Service (DoS) via a crafted GET request.	6.5	More Details
CVE-2023-24009	Auth. (subscriber+) Reflected Cross-site Scripting (XSS) vulnerability in Wpazure Themes Upfrontwp theme <= 1.1 versions.	6.5	More Details
CVE-2023-23828	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Swashata WP Category Post List Widget plugin <= 2.0.3 versions.	6.5	More Details
CVE-2023-23798	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Muneeb Layer Slider plugin <= 1.1.9.7 versions.	6.5	More Details
CVE-2023-40235	An NTLM Hash Disclosure was discovered in ArchiMate Archi before 5.1.0. When parsing the XMLNS value of an ArchiMate project file, if the namespace does not match the expected ArchiMate URL, the parser will access the provided resource. If the provided resource is a UNC path pointing to a share server that does not accept a guest account, the host will try to authenticate on the share by using the current user's session. NOTE: this issue occurs because Archi uses an unsafe configuration of the Eclipse Modeling Framework.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38209	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by an Incorrect Authorization vulnerability that could lead to a Security feature bypass. A low-privileged attacker could leverage this vulnerability to access other user's data. Exploitation of this issue does not require user interaction.	6.5	More Details
CVE-2023-23826	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Arsham Mirshah Add Posts to Pages plugin <= 1.4.1 versions.	6.5	More Details
CVE-2023-24393	Auth. (editor+) Stored Cross-Site Scripting (XSS) vulnerability in Sk. Abul Hasan Animated Number Counters plugin <= 1.6 versions.	6.5	More Details
CVE-2023-39965	1Panel is an open source Linux server operation and maintenance management panel. In version 1.4.3, authenticated attackers can download arbitrary files through the API interface. This code has unauthorized access. Attackers can freely download the file content on the target system. This may cause a large amount of information leakage. Version 1.5.0 has a patch for this issue.	6.5	More Details
CVE-2023-24471	An access control vulnerability was found, due to the restrictions that are applied on actual assertions not being enforced in their debug functionality. An authenticated user with reduced visibility can obtain unauthorized information via the debug functionality, obtaining data that would normally be not accessible in the Query and Assertions functions.	6.5	More Details
CVE-2023-39531	Sentry is an error tracking and performance monitoring platform. Starting in version 10.0.0 and prior to version 23.7.2, an attacker with sufficient client-side exploits could retrieve a valid access token for another user during the OAuth token exchange due to incorrect credential validation. The client ID must be known and the API application must have already been authorized on the targeted user account. Sentry SaaS customers do not need to take any action. Self-hosted installations should upgrade to version 23.7.2 or higher. There are no direct workarounds, but users should review applications authorized on their account and remove any that are no longer needed.	6.5	More Details
CVE-2023-39952	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 22.0.0 and prior to versions 22.2.10.13, 23.0.12.8, 24.0.12.4, 25.0.8, 26.0.3, and 27.0.1, a user can access files inside a subfolder of a groupfolder accessible to them, even if advanced permissions would block access to the subfolder. Nextcloud Server versions 25.0.8, 26.0.3, and 27.0.1 and Nextcloud Enterprise Server versions 22.2.10.13, 23.0.12.8, 24.0.12.4, 25.0.8, 26.0.3, and 27.0.1 contain a patch for this issue. No known workarounds are available.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23347	HCL DRYiCE iAutomate is affected by the use of a broken cryptographic algorithm. An attacker can potentially compromise the confidentiality and integrity of sensitive information.	6.4	More Details
CVE-2023-4265	Potential buffer overflow vulnerabilities in the following locations: https://github.com/zephyrproject-rtos/zephyr/blob/main/drivers/usb/device/usb_dc_native_posix.c#L359 https://github.com/zephyrproject-rtos/zephyr/blob/main/drivers/usb/device/usb_dc_native_posix.c#L359 https://github.com/zephyrproject-rtos/zephyr/blob/main/subsys/usb/device/class/netusb/function_rndis... https://github.com/zephyrproject-rtos/zephyr/blob/main/subsys/usb/device/class/netusb/function_rndis.c#L841	6.4	More Details
CVE-2023-4283	The EmbedPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'embedpress_calendar' shortcode in versions up to, and including, 3.8.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-32267	A potential vulnerability has been identified in OpenText / Micro Focus ArcSight Management Center. The vulnerability could be remotely exploited.	6.4	More Details
CVE-2023-22843	An authenticated attacker with administrative access to the web management interface can inject malicious JavaScript code inside the definition of a Threat Intelligence rule, that will be stored and can later be executed by another legitimate user viewing the details of such a rule. Via stored Cross-Site Scripting (XSS), an attacker may be able to perform unauthorized actions on behalf of legitimate users and/or gather sensitive information. JavaScript injection was possible in the contents for Yara rules, while limited HTML injection has been proven for packet and STYX rules.	6.4	More Details
CVE-2023-23346	HCL DRYiCE MyCloud is affected by the use of a broken cryptographic algorithm. An attacker can potentially compromise the confidentiality and integrity of sensitive information.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36671	An issue was discovered in the Clario VPN client through 5.9.1.1662 for macOS. The VPN client insecurely configures the operating system such that all IP traffic to the VPN server's IP address is sent in plaintext outside the VPN tunnel even if this traffic is not generated by the VPN client. This allows an adversary to trick the victim into sending plaintext traffic to the VPN server's IP address and thereby deanonymize the victim. NOTE: the tunnelcrack.mathyvanhoef.com website uses this CVE ID to refer more generally to "ServerIP attack for only traffic to the real IP address of the VPN server" rather than to only Clario.	6.3	More Details
CVE-2023-4106	Mattermost fails to check if the requesting user is a guest before performing different actions to public playbooks, resulting a guest being able to view, join, edit, export and archive public playbooks.	6.3	More Details
CVE-2023-38333	Zoho ManageEngine Applications Manager through 16530 allows reflected XSS while logged in.	6.1	More Details
CVE-2023-40224	MISP 2.4.174 allows XSS in app/View/Events/index.ctp.	6.1	More Details
CVE-2023-36314	There is a Cross Site Scripting (XSS) vulnerability in the value-text-o_sms_email_request_message parameters of index.php in PHPJabbers Callback Widget v1.0.	6.1	More Details
CVE-2023-38998	An open redirect in the Login page of OPNsense Community Edition before 23.7 and Business Edition before 23.4.2 allows attackers to redirect a victim user to an arbitrary web site via a crafted URL.	6.1	More Details
CVE-2022-4953	The Elementor Website Builder WordPress plugin before 3.5.5 does not filter out user-controlled URLs from being loaded into the DOM. This could be used to inject rogue iframes that point to malicious URLs.	6.1	More Details
CVE-2023-2803	The Ultimate Addons for Contact Form 7 WordPress plugin before 3.1.29 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-2022-38083	Improper initialization in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	6.1	More Details
CVE-2023-39000	A reflected cross-site scripting (XSS) vulnerability in the component /ui/diagnostics/log/core/ of OPNsense Community Edition before 23.7 and Business Edition before 23.4.2 allows attackers to inject arbitrary JavaScript via the URL path.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38347	An issue was discovered in LWsystems Benno MailArchiv 2.10.1. Attackers can cause XSS via JavaScript content to a mailbox.	6.1	More Details
CVE-2023-36313	PHPJabbers Document Creator v1.0 is vulnerable to Cross Site Scripting (XSS) via all post parameters of "Export Requests" aside from "request_feed".	6.1	More Details
CVE-2023-39002	A cross-site scripting (XSS) vulnerability in the act parameter of system_certmanager.php in OPNsense Community Edition before 23.7 and Business Edition before 23.4.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2023-39950	efibootguard is a simple UEFI boot loader with support for safely switching between current and updated partition sets. Insufficient or missing validation and sanitization of input from untrustworthy bootloader environment files can cause crashes and probably also code injections into `bg_setenv`) or programs using `libebgenv`. This is triggered when the affected components try to modify a manipulated environment, in particular its user variables. Furthermore, `bg_printenv` may crash over invalid read accesses or report invalid results. Not affected by this issue is EFI Boot Guard's bootloader EFI binary. EFI Boot Guard release v0.15 contains required patches to sanitize and validate the bootloader environment prior to processing it in userspace. Its library and tools should be updated, so should programs statically linked against it. An update of the bootloader EFI executable is not required. The only way to prevent the issue with an unpatched EFI Boot Guard version is to avoid accesses to user variables, specifically modifications to them.	6.1	More Details
CVE-2023-36309	There is a Cross Site Scripting (XSS) vulnerability in the "action" parameter of index.php in PHPJabbers Document Creator v1.0.	6.1	More Details
CVE-2023-36315	There is a Cross Site Scripting (XSS) vulnerability in the "action" parameter of index.php in PHPJabbers Callback Widget v1.0.	6.1	More Details
CVE-2023-4321	Cross-site Scripting (XSS) - Stored in GitHub repository cockpit-hq/cockpit prior to 2.4.3.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23208	Genesys Administrator Extension (GAX) before 9.0.105.15 is vulnerable to Cross Site Scripting (XSS) via the Business Structure page of the iWD plugin, aka GAX-11261.	6.1	More Details
CVE-2023-36310	There is a Cross Site Scripting (XSS) vulnerability in the "column" parameter of index.php in PHPJabbers Document Creator v1.0.	6.1	More Details
CVE-2020-24872	Cross Site Scripting (XSS) vulnerability in backend/pages/modify.php in Lepton-CMS version 4.7.0, allows remote attackers to execute arbitrary code.	6.1	More Details
CVE-2021-27524	Cross Site Scripting (XSS) vulnerability in margox braft-editor version 2.3.8, allows remote attackers to execute arbitrary code via the embed media feature.	6.1	More Details
CVE-2023-27887	Improper initialization in BIOS firmware for some Intel(R) NUCs may allow a privileged user to potentially enable information disclosure via local access.	6.1	More Details
CVE-2020-19952	Cross Site Scripting (XSS) vulnerability in Rendering Engine in jbt Markdown Editor thru commit 2252418c27dffbb35147acd8ed324822b8919477, allows remote attackers to execute arbirary code via crafted payload or opening malicious .md file.	6.1	More Details
CVE-2020-24075	Cross Site Scripting (XSS) vulnerability in Name Input Field in Contact Us form in Laborator Kalium before 3.0.4, allows remote attackers to execute arbitrary code.	6.1	More Details
CVE-2020-20523	Cross Site Scripting (XSS) vulnerability in adm_user parameter in Gila CMS version 1.11.3, allows remote attackers to execute arbitrary code during the Gila CMS installation.	6.1	More Details
CVE-2020-27449	Cross Site Scripting (XSS) vulnerability in Query Report feature in Zoho ManageEngine Password Manager Pro version 11001, allows remote attackers to execute arbitrary code and steal cookies via crafted JavaScript payload.	6.1	More Details
CVE-2020-28717	Cross Site Scripting (XSS) vulnerability in content1 parameter in demo.jsp in kindsoft kindeditor version 4.1.12, allows attackers to execute arbitrary code.	6.1	More Details
CVE-2023-22330	Use of uninitialized resource in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable information disclosure via local access.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22356	Improper initialization in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable information disclosure via local access.	6.0	More Details
CVE-2023-4273	A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged attacker could use this flaw to overflow the kernel stack.	6.0	More Details
CVE-2023-22444	Improper initialization in some Intel(R) NUC 13 Extreme Compute Element, Intel(R) NUC 13 Extreme Kit, Intel(R) NUC 11 Performance Kit, Intel(R) NUC 11 Performance Mini PC, Intel(R) NUC Compute Element, Intel(R) NUC Laptop Kit, Intel(R) NUC Pro Kit, Intel(R) NUC Pro Board and Intel(R) NUC Pro Mini PC BIOS firmware may allow a privileged user to potentially enable information disclosure via local access.	6.0	More Details
CVE-2022-34657	Improper input validation in firmware for some Intel(R) PCSD BIOS before version 02.01.0013 may allow a privileged user to potentially enable information disclosure via local access.	6.0	More Details
CVE-2023-23908	Improper access control in some 3rd Generation Intel(R) Xeon(R) Scalable processors may allow a privileged user to potentially enable information disclosure via local access.	6.0	More Details
CVE-2023-32285	Improper access control in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable denial of service via local access.	6.0	More Details
CVE-2023-40253	Improper Authentication vulnerability in Genians Genian NAC V4.0, Genians Genian NAC V5.0, Genians Genian NAC Suite V5.0, Genians Genian ZTNA allows Authentication Abuse.This issue affects Genian NAC V4.0: from V4.0.0 through V4.0.155; Genian NAC V5.0: from V5.0.0 through V5.0.42 (Revision 117460); Genian NAC Suite V5.0: from V5.0.0 through V5.0.54; Genian ZTNA: from V6.0.0 through V6.0.15.	6.0	More Details
CVE-2023-30477	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Essitco AFFILIATE Solution plugin <= 1.0 versions.	5.9	More Details
CVE-2023-30751	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in iControlWP Article Directory Redux plugin <= 1.0.2 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29097	Auth. (author+) Stored Cross-Site Scripting (XSS) vulnerability in a3rev Software a3 Portfolio plugin <= 3.1.0 versions.	5.9	More Details
CVE-2023-30749	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in ihomefinder Optima Express + MarketBoost IDX Plugin plugin <= 7.3.0 versions.	5.9	More Details
CVE-2023-30752	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Silvia Pfeiffer and Andrew Nimmo External Videos plugin <= 2.0.1 versions.	5.9	More Details
CVE-2023-38397	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Eggemplo Gestion-Pymes plugin <= 1.5.6 versions.	5.9	More Details
CVE-2023-34374	Auth. (editor+) Stored Cross-Site Scripting (XSS) vulnerability in Rahul Aryan AnsPress plugin <= 4.3.0 versions.	5.9	More Details
CVE-2022-44629	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Catalyst Connect Catalyst Connect Zoho CRM Client Portal plugin <= 2.0.0 versions.	5.9	More Details
CVE-2023-37388	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Sudipto Pratap Mahato Simple Light Weight Social Share plugin <= 2.0 versions.	5.9	More Details
CVE-2023-23871	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Webdzier Button plugin <= 1.1.23 versions.	5.9	More Details
CVE-2023-40012	uthenticode is a small cross-platform library for partially verifying Authenticode digital signatures. Versions of uthenticode prior to the 2.x series did not check Extended Key Usages in certificates, in violation of the Authenticode X.509 certificate profile. As a result, a malicious user could produce a "signed" PE file that uthenticode would verify and consider valid using an X.509 certificate that isn't entitled to produce code signatures (e.g., a SSL certificate). By design, uthenticode does not perform full-chain validation. However, the absence of EKU validation was an unintended oversight. The 2.0.0 release series includes EKU checks. There are no workarounds to this vulnerability.	5.9	More Details
CVE-2023-36530	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Smartypants SP Project & Document Manager plugin <= 4.67 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24389	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in brandiD Social Proof (Testimonial) Slider plugin <= 2.2.3 versions.	5.9	More Details
CVE-2023-24391	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Spider Teams ApplyOnline plugin <= 2.5 versions.	5.9	More Details
CVE-2023-23900	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in YIKES, Inc. Easy Forms for Mailchimp plugin <= 6.8.8 versions.	5.8	More Details
CVE-2023-39958	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 22.0.0 and prior to versions 22.2.10.13, 23.0.12.8, 24.0.12.5, 25.0.9, 26.0.4, and 27.0.1, missing protection allows an attacker to brute force the client secrets of configured OAuth2 clients. Nextcloud Server versions 25.0.9, 26.0.4, and 27.0.1 and Nextcloud Enterprise Server versions 22.2.10.13, 23.0.12.8, 24.0.12.5, 25.0.9, 26.0.4, and 27.0.1 contain a patch for this issue. No known workarounds are available.	5.8	More Details
CVE-2023-35838	The WireGuard client 0.5.3 on Windows insecurely configures the operating system and firewall such that traffic to a local network that uses non-RFC1918 IP addresses is blocked. This allows an adversary to trick the victim into blocking IP traffic to selected IP addresses and services even while the VPN is enabled. NOTE: the tunnelcrack.mathyvanhoef.com website uses this CVE ID to refer more generally to "LocalNet attack resulting in the blocking of traffic" rather than to only WireGuard.	5.7	More Details
CVE-2023-36672	An issue was discovered in the Clario VPN client through 5.9.1.1662 for macOS. The VPN client insecurely configures the operating system such that traffic to the local network is sent in plaintext outside the VPN tunnel even if the local network is using a non-RFC1918 IP subnet. This allows an adversary to trick the victim into sending arbitrary IP traffic in plaintext outside the VPN tunnel. NOTE: the tunnelcrack.mathyvanhoef.com website uses this CVE ID to refer more generally to "LocalNet attack resulting in leakage of traffic in plaintext" rather than to only Clario.	5.7	More Details
CVE-2023-28736	Buffer overflow in some Intel(R) SSD Tools software before version mdadm-4.2-rc2 may allow a privileged user to potentially enable escalation of privilege via local access.	5.7	More Details
CVE-2023-25775	Improper access control in the Intel(R) Ethernet Controller RDMA driver for linux before version 1.9.30 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22655	An access issue was addressed with improvements to the sandbox. This issue is fixed in macOS Monterey 12.3, iOS 15.4 and iPadOS 15.4. An app may be able to leak sensitive user information.	5.5	More Details
CVE-2023-38230	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free 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-2023-21292	In openContentUri of ActivityManagerService.java, there is a possible way for a third party app to obtain restricted files due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2022-26699	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13. An app may be able to cause a denial-of-service to Endpoint Security clients.	5.5	More Details
CVE-2022-46722	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2023-38232	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-27939	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3. Processing an image may result in disclosure of process memory.	5.5	More Details
CVE-2023-21288	In visitUris of Notification.java, there is a possible way to reveal images across users due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-38235	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22646	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Monterey 12.2. A malicious application may be able to modify protected parts of the file system.	5.5	More Details
CVE-2020-24221	An issue was discovered in GetByte function in miniupnp ngiflib version 0.4, allows local attackers to cause a denial of service (DoS) via crafted .gif file (infinite loop).	5.5	More Details
CVE-2023-21268	In update of MmsProvider.java, there is a possible way to change directory permissions due to a path traversal error. This could lead to local denial of service of SIM recognition with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-38210	Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-21277	In visitUris of RemoteViews.java, there is a possible way to reveal images across users due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21234	In launchConfirmationActivity of ChooseLockSettingsHelper.java, there is a possible way to enable developer options without the lockscreen PIN due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21230	In onAccessPointChanged of AccessPointPreference.java, there is a possible way for unprivileged apps to receive a broadcast about WiFi access point change and its BSSID or SSID due to a precondition check failure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-38237	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21271	In parseInputs of ShimPreparedModel.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21274	In convertSubgraphFromHAL of ShimConverter.cpp, 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.	5.5	More Details
CVE-2023-21276	In writeToParcel of CursorWindow.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21279	In visitUris of RemoteViews.java, there is a possible cross-user media read due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-29303	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use After Free 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-2023-21280	In setMediaButtonBroadcastReceiver of MediaSessionRecord.java, there is a possible permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21283	In multiple functions of StatusHints.java, there is a possible way to reveal images across users due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	5.5	More Details
CVE-2023-21284	In multiple functions of DevicePolicyManager.java, there is a possible way to prevent enabling the Find my Device feature due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21285	In setMetadata of MediaSessionRecord.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21267	In multiple functions of KeyguardViewMediator.java, there is a possible way to bypass lockdown mode with screen pinning due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-30698	Improper access control vulnerability in TelephonyUI prior to SMR Aug-2023 Release 1 allows local attacker to connect BLE without privilege.	5.5	More Details
CVE-2023-38236	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-21289	In multiple locations, there is a possible bypass of a multi user security boundary due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-38238	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free 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-2023-4333	Broadcom RAID Controller web interface doesn’t enforce SSL cipher ordering by server	5.5	More Details
CVE-2023-38239	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-38850	Buffer Overflow vulnerability in Michaelrsweet codedoc v.3.7 allows an attacker to cause a denial of service via the codedoc.c:1742 comppnent.	5.5	More Details
CVE-2022-44612	Use of hard-coded credentials in some Intel(R) Unison(TM) software before version 10.12 may allow an authenticated user user to potentially enable information disclosure via local access.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27506	Improper buffer restrictions in the Intel(R) Optimization for Tensorflow software before version 2.12 may allow an authenticated user to potentially enable escalation of privilege via local access.	5.5	More Details
CVE-2023-28711	Insufficient control flow management in the Hyperscan Library maintained by Intel(R) before version 5.4.1 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2023-38857	Buffer Overflow vulnerability infaad2 v.2.10.1 allows a remote attacker to execute arbitrary code and cause a denial of service via the stcoin function in mp4read.c.	5.5	More Details
CVE-2021-3236	vim 8.2.2348 is affected by null pointer dereference, allows local attackers to cause a denial of service (DoS) via the ex_buffer_all method.	5.5	More Details
CVE-2021-28429	Integer overflow vulnerability in av_timecode_make_string in libavutil/timecode.c in FFmpeg version 4.3.2, allows local attackers to cause a denial of service (DoS) via crafted .mov file.	5.5	More Details
CVE-2023-24478	Use of insufficiently random values for some Intel Agilex(R) software included as part of Intel(R) Quartus(R) Prime Pro Edition for linux before version 22.4 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2021-28025	Integer Overflow vulnerability in qsvghandler.cpp in Qt qtsvg versions 5.15.1, 6.0.0, 6.0.2, and 6.2, allows local attackers to cause a denial of service (DoS).	5.5	More Details
CVE-2023-38213	Adobe Dimension version 3.4.9 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-2020-36024	An issue was discovered in freedesktop poppler version 20.12.1, allows remote attackers to cause a denial of service (DoS) via crafted .pdf file to FoFiType1C::convertToType1 function.	5.5	More Details
CVE-2020-35990	Buffer Overflow vulnerability in cFilenameInit parameter in browseForDoc function in Foxit Software Foxit PDF Reader version 10.1.0.37527, allows local attackers to cause a denial of service (DoS) via crafted .pdf file.	5.5	More Details
CVE-2023-4328	Broadcom RAID Controller web interface is vulnerable to exposure of sensitive data and the keys used for encryption are accessible to any local user on Windows	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4327	Broadcom RAID Controller web interface is vulnerable to exposure of sensitive data and the keys used for encryption are accessible to any local user on Linux	5.5	More Details
CVE-2020-24187	An issue was discovered in ecma-helpers.c in jerryscript version 2.3.0, allows local attackers to cause a denial of service (DoS) (Null Pointer Dereference).	5.5	More Details
CVE-2023-30778	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Blubrry PowerPress Podcasting plugin by Blubrry plugin <= 10.0.1 versions.	5.5	More Details
CVE-2023-38840	Bitwarden Desktop 2023.7.0 and below allows an attacker with local access to obtain sensitive information via the Bitwarden.exe process.	5.5	More Details
CVE-2023-28199	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2023-38245	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted Microsoft Office file, or visit an attacker controlled web page.	5.5	More Details
CVE-2023-38247	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-38243	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free 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-2023-38242	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38248	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-27947	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3. Processing an image may result in disclosure of process memory.	5.5	More Details
CVE-2023-27948	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3. Processing an image may result in disclosure of process memory.	5.5	More Details
CVE-2023-38241	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-38244	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-40216	OpenBSD 7.3 before errata 014 is missing an argument-count bounds check in console terminal emulation. This could cause incorrect memory access and a kernel crash after receiving crafted DCS or CSI terminal escape sequences.	5.5	More Details
CVE-2023-21290	In update of MmsProvider.java, there is a possible way to bypass file permission checks due to a race condition. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-40360	QEMU through 8.0.4 accesses a NULL pointer in nvme_directive_receive in hw/nvme/ctrl.c because there is no check for whether an endurance group is configured before checking whether Flexible Data Placement is enabled.	5.5	More Details
CVE-2023-40305	GNU indent 2.2.13 has a heap-based buffer overflow in search_brace in indent.c via a crafted file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38240	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2020-28849	Cross Site Scripting (XSS) vulnerability in ChurchCRM version 4.2.1, allows remote attckers to execute arbitrary code and gain sensitive information via crafted payload in Add New Deposit field in View All Deposit module.	5.4	More Details
CVE-2020-25915	Cross Site Scripting (XSS) vulnerability in UserController.php in ThinkCMF version 5.1.5, allows attackers to execute arbitrary code via crafted user_login.	5.4	More Details
CVE-2023-38687	Svelecte is a flexible autocomplete/select component written in Svelte. Svelecte item names are rendered as raw HTML with no escaping. This allows the injection of arbitrary HTML into the Svelecte dropdown. This can be exploited to execute arbitrary JavaScript whenever a Svelecte dropdown is opened. Item names given to Svelecte appear to be directly rendered as HTML by the default item renderer. This means that any HTML tags in the name are rendered as HTML elements not as text. Note that the custom item renderer shown in https://mskocik.github.io/svelecte/#item-rendering is also vulnerable to the same exploit. Any site that uses Svelecte with dynamically created items either from an external source or from user-created content could be vulnerable to an XSS attack (execution of untrusted JavaScript), clickjacking or any other attack that can be performed with arbitrary HTML injection. The actual impact of this vulnerability for a specific application depends on how trustworthy the sources that provide Svelecte items are and the steps that the application has taken to mitigate XSS attacks. XSS attacks using this vulnerability are mostly mitigated by a Content Security Policy that blocks inline JavaScript. This issue has been addressed in version 3.16.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2023-36312	There is a Cross Site Scripting (XSS) vulnerability in the value-enum-o_bf_include_timezone parameter of index.php in PHPJabbers Callback Widget v1.0.	5.4	More Details
CVE-2023-37625	A stored cross-site scripting (XSS) vulnerability in Netbox v3.4.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Custom Link templates.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40024	ScanCode.io is a server to script and automate software composition analysis pipelines. In the `/license/` endpoint, the detailed view key is not properly validated and sanitized, which can result in a potential cross-site scripting (XSS) vulnerability when attempting to access a detailed license view that does not exist. Attackers can exploit this vulnerability to inject malicious scripts into the response generated by the `license_details_view` function. When unsuspecting users visit the page, their browsers will execute the injected scripts, leading to unauthorized actions, session hijacking, or stealing sensitive information. This issue has been addressed in release `32.5.2`. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.4	More Details
CVE-2023-0871	XXE injection in /rtc/post/ endpoint in OpenMNS Horizon 31.0.8 and versions earlier than 32.0.2 on multiple platforms is vulnerable to XML external entity (XXE) injection, which can be used for instance to force Horizon to make arbitrary HTTP requests to internal and external services. The solution is to upgrade to Meridian 2023.1.6, 2022.1.19, 2021.1.30, 2020.1.38 or Horizon 32.0.2 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. OpenNMS thanks Erik Wynter and Moshe Apelbaum for reporting this issue.	5.4	More Details
CVE-2023-4282	The EmbedPress plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'admin_post_remove' and 'remove_private_data' functions in versions up to, and including, 3.8.2. This makes it possible for authenticated attackers with subscriber privileges or above, to delete plugin settings.	5.4	More Details
CVE-2023-39006	The Crash Reporter (crash_reporter.php) component of OPNsense Community Edition before 23.7 and Business Edition before 23.4.2 mishandles input sanitization.	5.4	More Details
CVE-2023-4347	Cross-site Scripting (XSS) - Reflected in GitHub repository librenms/librenms prior to 23.8.0.	5.4	More Details
CVE-2023-38898	An issue in Python cpython v.3.7 allows an attacker to obtain sensitive information via the _asyncio._swap_current_task component. NOTE: this is disputed by the vendor because (1) neither 3.7 nor any other release is affected (it is a bug in some 3.12 pre-releases); (2) there are no common scenarios in which an adversary can call _asyncio._swap_current_task but does not already have the ability to call arbitrary functions; and (3) there are no common scenarios in which sensitive information, which is not already accessible to an adversary, becomes accessible through this bug.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4359	Inappropriate implementation in App Launcher in Google Chrome on iOS prior to 116.0.5845.96 allowed a remote attacker to potentially spoof elements of the security UI via a crafted HTML page. (Chromium security severity: Medium)	5.3	More Details
CVE-2023-4361	Inappropriate implementation in Autofill in Google Chrome on Android prior to 116.0.5845.96 allowed a remote attacker to bypass Autofill restrictions via a crafted HTML page. (Chromium security severity: Medium)	5.3	More Details
CVE-2023-30700	PendingIntent hijacking vulnerability in SemWifiApTimeOutImpl in framework prior to SMR Aug-2023 Release 1 allows local attackers to access ContentProvider without proper permission.	5.3	More Details
CVE-2023-32003	`fs.mkdtemp()` and `fs.mkdtempSync()` can be used to bypass the permission model check using a path traversal attack. This flaw arises from a missing check in the fs.mkdtemp() API and the impact is a malicious actor could create an arbitrary directory. This vulnerability affects all users using the experimental permission model in Node.js 20. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.	5.3	More Details
CVE-2023-3953	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause memory corruption when an authenticated user opens a tampered log file from GP-Pro EX.	5.3	More Details
CVE-2023-32656	Improper buffer restrictions in some Intel(R) RealSense(TM) ID software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	5.3	More Details
CVE-2022-27879	Improper buffer restrictions in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	5.3	More Details
CVE-2023-40014	OpenZeppelin Contracts is a library for secure smart contract development. Starting in version 4.0.0 and prior to version 4.9.3, contracts using `ERC2771Context` along with a custom trusted forwarder may see `_msgSender` return `address(0)` in calls that originate from the forwarder with calldata shorter than 20 bytes. This combination of circumstances does not appear to be common, in particular it is not the case for `MinimalForwarder` from OpenZeppelin Contracts, or any deployed forwarder the team is aware of, given that the signer address is appended to all calls that originate from these forwarders. The problem has been patched in v4.9.3.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29500	Exposure of sensitive information to an unauthorized actor in BIOS firmware for some Intel(R) NUCs may allow a privilege user to potentially enable information disclosure via local access.	5.3	More Details
CVE-2021-25786	An issue was discovered in QPDF version 10.0.4, allows remote attackers to execute arbitrary code via crafted .pdf file to Pl_ASCII85Decoder::write parameter in libqpdf.	5.3	More Details
CVE-2023-39387	Vulnerability of permission control in the window management module. Successful exploitation of this vulnerability may cause malicious pop-up windows.	5.3	More Details
CVE-2023-34427	Protection mechanism failure in some Intel(R) RealSense(TM) ID software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	5.3	More Details
CVE-2023-32609	Improper access control in the Intel Unite(R) android application before version 4.2.3504 may allow an authenticated user to potentially enable information disclosure via local access.	5.0	More Details
CVE-2023-23903	An authenticated administrator can upload a SAML configuration file with the wrong format, with the application not checking the correct file format. Every subsequent application request will return an error. The whole application in rendered unusable until a console intervention.	4.9	More Details
CVE-2023-40028	Ghost is an open source content management system. Versions prior to 5.59.1 are subject to a vulnerability which allows authenticated users to upload files that are symlinks. This can be exploited to perform an arbitrary file read of any file on the host operating system. Site administrators can check for exploitation of this issue by looking for unknown symlinks within Ghost's `content/` folder. Version 5.59.1 contains a fix for this issue. All users are advised to upgrade. There are no known workarounds for this vulnerability.	4.9	More Details
CVE-2023-37858	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password.	4.9	More Details
CVE-2021-25856	An issue was discovered in pcmt superMicro-CMS version 3.11, allows attackers to delete files via crafted image file in images.php.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2606	The WP Brutal AI WordPress plugin before 2.06 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-2023-37070	Code Projects Hospital Information System 1.0 is vulnerable to Cross Site Scripting (XSS)	4.8	More Details
CVE-2023-39953	user_oidc provides the OIDC connect user backend for Nextcloud, an open-source cloud platform. Starting in version 1.0.0 and prior to version 1.3.3, missing verification of the issuer would have allowed an attacker to perform a man-in-the-middle attack returning corrupted or known token they also have access to. user_oidc 1.3.3 contains a patch. No known workarounds are available.	4.8	More Details
CVE-2023-3645	The Contact Form Builder by Bit Form WordPress plugin before 2.2.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-3937	Cross site scripting vulnerability in web portal in Snow Software License Manager from version 9.0.0 up to and including 9.30.1 on Windows allows an authenticated user with high privileges to trigger cross site scripting attack via the web browser	4.8	More Details
CVE-2023-2802	The Ultimate Addons for Contact Form 7 WordPress plugin before 3.1.29 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-3721	The WP-EMail WordPress plugin before 2.69.1 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-2023-3328	The Custom Field For WP Job Manager WordPress plugin before 1.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-27861	Unauth. Open Redirect vulnerability in Arscode Ninja Popups plugin <= 4.7.5 versions.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29299	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Untrusted Search Path vulnerability that could lead to Application denial-of-service. An attacker could leverage this vulnerability if the default PowerShell Set-ExecutionPolicy is set to Unrestricted, making the attack complexity high. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4.7	More Details
CVE-2023-30701	PendingIntent hijacking in WifiGeofenceManager prior to SMR Aug-2023 Release 1 allows local attacker to arbitrary file access.	4.7	More Details
CVE-2023-31450	A path traversal vulnerability was identified in the SQL v2 sensors in PRTG 23.2.84.1566 and earlier versions where an authenticated user with write permissions could trick the SQL v2 sensors into behaving differently for existing files and non-existing files. This made it possible to traverse paths, allowing the sensor to execute files outside the designated custom sensors folder. The severity of this vulnerability is medium and received a score of 4.7 CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L	4.7	More Details
CVE-2023-31449	A path traversal vulnerability was identified in the WMI Custom sensor in PRTG 23.2.84.1566 and earlier versions where an authenticated user with write permissions could trick the WMI Custom sensor into behaving differently for existing files and non-existing files. This made it possible to traverse paths, allowing the sensor to execute files outside the designated custom sensors folder. The severity of this vulnerability is medium and received a score of 4.7 CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L	4.7	More Details
CVE-2023-31448	A path traversal vulnerability was identified in the HL7 sensor in PRTG 23.2.84.1566 and earlier versions where an authenticated user with write permissions could trick the HL7 sensor into behaving differently for existing files and non-existing files. This made it possible to traverse paths, allowing the sensor to execute files outside the designated custom sensors folder. The severity of this vulnerability is medium and received a score of 4.7 CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L	4.7	More Details
CVE-2023-39841	Missing encryption in the RFID tag of Etekcity 3-in-1 Smart Door Lock v1.0 allows attackers to create a cloned tag via brief physical proximity to the original device.	4.6	More Details
CVE-2023-34349	Race condition in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4108	Mattermost fails to sanitize post metadata during audit logging resulting in permalinks contents being logged	4.5	More Details
CVE-2023-33867	Improper buffer restrictions in some Intel(R) RealSense(TM) ID software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	4.4	More Details
CVE-2023-29243	Unchecked return value in some Intel(R) RealSense(TM) ID software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow a priviledged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2023-27392	Incorrect default permissions in the Intel(R) Support android application before version v23.02.07 may allow a privileged user to potentially enable information disclosure via local access.	4.4	More Details
CVE-2023-22338	Out-of-bounds read in some Intel(R) oneVPL GPU software before version 22.6.5 may allow an authenticated user to potentially enable information disclosure via local access.	4.4	More Details
CVE-2022-41984	Protection mechanism failure for some Intel(R) Arc(TM) graphics cards A770 and A750 Limited Edition sold between October of 2022 and December of 2022 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2023-30681	An improper input validation vulnerability within initialize function in HAL VaultKeeper prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write.	4.4	More Details
CVE-2023-30696	An improper input validation in IpcTxGetVerifyAkey in libsec-ril prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write.	4.4	More Details
CVE-2023-30697	An improper input validation in IpcTxCfgSetSimlockPayload in libsec-ril prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write.	4.4	More Details
CVE-2023-20560	Insufficient validation of the IOCTL (Input Output Control) input buffer in AMD Ryzen™ Master may allow a privileged attacker to provide a null value potentially resulting in a Windows crash leading to denial of service.	4.4	More Details
CVE-2023-30683	Improper access control in Telecom prior to SMR Aug-2023 Release 1 allows local attackers to call endCall API without permission.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30685	Improper access control vulnerability in Telecom prior to SMR Aug-2023 Release 1 allows local attakcers to change TTY mode.	4.3	More Details
CVE-2023-30684	Improper access control in Samsung Telecom prior to SMR Aug-2023 Release 1 allows local attackers to call acceptRingingCall API without permission.	4.3	More Details
CVE-2022-46725	A spoofing issue existed in the handling of URLs. This issue was addressed with improved input validation. This issue is fixed in iOS 16.4 and iPadOS 16.4. Visiting a malicious website may lead to address bar spoofing.	4.3	More Details
CVE-2022-36351	Improper input validation in some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi software may allow an unauthenticated user to potentially enable denial of service via adjacent access.	4.3	More Details
CVE-2023-4242	The FULL - Customer plugin for WordPress is vulnerable to Information Disclosure via the /health REST route in versions up to, and including, 2.2.3 due to improper authorization. This allows authenticated attackers with subscriber-level permissions and above to obtain sensitive information about the site configuration as disclosed by the WordPress health check.	4.3	More Details
CVE-2023-24015	A partial DoS vulnerability has been detected in the Reports section, exploitable by a malicious authenticated user forcing a report to be saved with its name set as null. The reports section will be partially unavailable for all later attempts to use it, with the report list seemingly stuck on loading.	4.3	More Details
CVE-2023-30682	Improper access control in Telecom prior to SMR Aug-2023 Release 1 allows local attackers to call silenceRinger API without permission.	4.3	More Details
CVE-2023-4360	Inappropriate implementation in Color in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-37856	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog within the embedded Qt browser .	4.3	More Details
CVE-2023-3601	The Simple Author Box WordPress plugin before 2.52 does not verify a user ID before outputting information about that user, leading to arbitrary user information disclosure to users with a role as low as Contributor.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38752	Improper authorization vulnerability in Special Interest Group Network for Analysis and Liaison versions 4.4.0 to 4.7.7 allows the authorized API users to view the attribute information of the poster that is set as"non-disclosure" in the system settings.	4.3	More Details
CVE-2023-40292	Harman Infotainment 20190525031613 and later discloses the IP address via CarPlay CTRL packets.	4.3	More Details
CVE-2023-4363	Inappropriate implementation in WebShare in Google Chrome on Android prior to 116.0.5845.96 allowed a remote attacker to spoof the contents of a dialog URL via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-4364	Inappropriate implementation in Permission Prompts in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-4365	Inappropriate implementation in Fullscreen in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-38751	Improper authorization vulnerability in Special Interest Group Network for Analysis and Liaison versions 4.4.0 to 4.7.7 allows the authorized API users to view the organization information of the information receiver that is set as "non-disclosure" in the information provision operation.	4.3	More Details
CVE-2023-37855	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser.	4.3	More Details
CVE-2023-25182	Uncontrolled search path element in the Intel(R) Unite(R) Client software for Mac before version 4.2.11 may allow an authenticated user to potentially enable escalation of privilege via local access.	4.2	More Details
CVE-2022-43505	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable denial of service via local access.	4.1	More Details
CVE-2022-38076	Improper input validation in some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi software may allow an authenticated user to potentially enable escalation of privilege via local access.	3.8	More Details
CVE-2023-37857	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. These session-cookies created by the attacker are not sufficient to obtain a valid session on the device.	3.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39954	user_oidc provides the OIDC connect user backend for Nextcloud, an open-source cloud platform. Starting in version 1.0.0 and prior to version 1.3.3, an attacker that obtained at least read access to a snapshot of the database can impersonate the Nextcloud server towards linked servers. user_oidc 1.3.3 contains a patch. No known workarounds are available.	3.8	More Details
CVE-2023-4304	Business Logic Errors in GitHub repository froxlor/froxlor prior to 2.0.22,2.1.0.	3.8	More Details
CVE-2023-30704	Improper Authorization vulnerability in Samsung Internet prior to version 22.0.0.35 allows physical attacker access downloaded files in Secret Mode without user authentication.	3.8	More Details
CVE-2023-40027	Keystone is an open source headless CMS for Node.js — built with GraphQL and React. When `ui.isAccessAllowed` is set as `undefined`, the `adminMeta` GraphQL query is publicly accessible (no session required). This is different to the behaviour of the default AdminUI middleware, which by default will only be publicly accessible (no session required) if a `session` strategy is not defined. This vulnerability does not affect developers using the `@keystone-6/auth` package, or any users that have written their own `ui.isAccessAllowed` (that is to say, `isAccessAllowed` is not `undefined`). This vulnerability does affect users who believed that their `session` strategy will, by default, enforce that `adminMeta` is inaccessible by the public in accordance with that strategy; akin to the behaviour of the AdminUI middleware. This vulnerability has been patched in `@keystone-6/core` version `5.5.1`. Users are advised to upgrade. Users unable to upgrade may opt to write their own `isAccessAllowed` functionality to work-around this vulnerability.	3.7	More Details
CVE-2023-39955	Notes is a note-taking app for Nextcloud, an open-source cloud platform. Starting in version 4.4.0 and prior to version 4.8.0, when creating a note file with HTML, the content is rendered in the preview instead of the file being offered to download. Nextcloud Notes app version 4.8.0 contains a patch for the issue. No known workarounds are available.	3.5	More Details
CVE-2023-39959	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.9, 26.0.4, and 27.0.1, unauthenticated users could send a DAV request which reveals whether a calendar or an address book with the given identifier exists for the victim. Nextcloud Server versions 25.0.9, 26.0.4, and 27.0.1 and Nextcloud Enterprise Server versions 25.0.9, 26.0.4, and 27.0.1 contain a patch for this issue. No known workarounds are available.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39961	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 24.0.4 and prior to versions 25.0.9, 26.0.4, and 27.0.1, when a folder with images or an image was shared without download permissions, the user could add the image inline into a text file and download it. Nextcloud Server versions 25.0.9, 26.0.4, and 27.0.1 and Nextcloud Enterprise Server versions 24.0.12.5, 25.0.9, 26.0.4, and 27.0.1 contain a patch for this issue. No known workarounds are available.	3.5	More Details
CVE-2023-37511	If certain App Transport Security (ATS) settings are set in a certain manner, insecure loading of web content can be achieved.	3.5	More Details
CVE-2023-4371	A vulnerability was found in phpRecDB 1.3.1. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument r/view leads to cross site scripting. The attack may be launched remotely. VDB-237194 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-28938	Uncontrolled resource consumption in some Intel(R) SSD Tools software before version mdadm-4.2-rc2 may allow a priviledged user to potentially enable denial of service via local access.	3.4	More Details
CVE-2023-39341	"FFRI yarai", "FFRI yarai Home and Business Edition" and their OEM products handle exceptional conditions improperly, which may lead to denial-of-service (DoS) condition. Affected products and versions are as follows: FFRI yarai versions 3.4.0 to 3.4.6 and 3.5.0, FFRI yarai Home and Business Edition version 1.4.0, InfoTrace Mark II Malware Protection (Mark II Zerona) versions 3.0.1 to 3.2.2, Zerona / Zerona PLUS versions 3.2.32 to 3.2.36, ActSecure χ versions 3.4.0 to 3.4.6 and 3.5.0, Dual Safe Powered by FFRI yarai version 1.4.1, EDR Plus Pack (Bundled FFRI yarai versions 3.4.0 to 3.4.6 and 3.5.0), and EDR Plus Pack Cloud (Bundled FFRI yarai versions 3.4.0 to 3.4.6 and 3.5.0).	3.3	More Details
CVE-2023-22840	Improper neutralization in software for the Intel(R) oneVPL GPU software before version 22.6.5 may allow an authenticated user to potentially enable denial of service via local access.	3.3	More Details
CVE-2023-21278	In multiple locations, there is a possible way to obscure the microphone privacy indicator 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.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21232	In multiple locations, there is a possible way to retrieve sensor data without permissions due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2023-30703	Improper URL validation vulnerability in Samsung Members prior to version 14.0.07.1 allows attackers to access sensitive information.	3.3	More Details
CVE-2023-33877	Out-of-bounds write in some Intel(R) RealSense(TM) ID software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	3.3	More Details
CVE-2023-30760	Out-of-bounds read in some Intel(R) RealSense(TM) ID software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow an authenticated user to potentially enable information disclosure via local access.	3.3	More Details
CVE-2022-32876	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13. A shortcut may be able to view the hidden photos album without authentication.	3.3	More Details
CVE-2022-38973	Improper access control for some Intel(R) Arc(TM) graphics cards A770 and A750 Limited Edition sold between October of 2022 and December of 2022 may allow an authenticated user to potentially enable denial of service or infomation disclosure via local access.	3.3	More Details
CVE-2023-37513	When the app is put to the background and the user goes to the task switcher of iOS, the app snapshot is not blurred which may reveal sensitive information.	3.3	More Details
CVE-2023-37512	When the app is put to the background and the user goes to the task switcher of iOS, the app snapshot is not blurred which may reveal sensitive information.	3.3	More Details
CVE-2023-39418	A vulnerability was found in PostgreSQL with the use of the MERGE command, which fails to test new rows against row security policies defined for UPDATE and SELECT. If UPDATE and SELECT policies forbid some rows that INSERT policies do not forbid, a user could store such rows.	3.1	More Details
CVE-2023-4105	Mattermost fails to delete the attachments when deleting a message in a thread allowing a simple user to still be able to access and download the attachment of a deleted message	3.1	More Details
CVE-2023-39842	Missing encryption in the RFID tag of Digoo DG-HAMB Smart Home Security System v1.0 allows attackers to create a cloned tag via brief physical proximity to the original device.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39843	Missing encryption in the RFID tag of Suleve 5-in-1 Smart Door Lock v1.0 allows attackers to create a cloned tag via brief physical proximity to the original device.	2.4	More Details
CVE-2022-46724	This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 16.4 and iPadOS 16.4. A person with physical access to an iOS device may be able to view the last image used in Magnifier from the lock screen.	2.4	More Details
CVE-2023-4275	Rejected reason: It is invalid.	N/A	More Details
CVE-2023-4330	Rejected reason: Broadcom were unable to duplicate the attack as described by Intel DCG Team.	N/A	More Details
CVE-2023-39848	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-4128	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-4206, CVE-2023-4207, CVE-2023-4208. Reason: This record is a duplicate of CVE-2023-4206, CVE-2023-4207, CVE-2023-4208. Notes: All CVE users should reference CVE-2023-4206, CVE-2023-4207, CVE-2023-4208 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2022-3403	Rejected reason: Duplicate, please use CVE-2023-28931 instead.	N/A	More Details
CVE-2023-39849	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details